h e g

Haute école de gestion
Genève

Operational risk management in the digital era in the Swiss banking industry

Bachelor Project submitted for the degree of
Bachelor of Science HES in International Business Management

by

Romain GIMBLETT

Bachelor Project Advisor:

Christophe COURBAGE, Professor at the Haute Ecole de Gestion de Genève

Geneva, Friday 1st of June 2018
Haute Ecole de Gestion de Genève (HEG-GE)
International Business Management

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

Declaration

This Bachelor Project is submitted as part of the final examination requirements of the Haute Ecole de Gestion de Genève, for the Bachelor of Science HES-SO in International Business Management.

The student accepts the terms of the confidentiality agreement if one has been signed. The use of any conclusions or recommendations made in the Bachelor Project, with no prejudice to their value, engages neither the responsibility of the author, nor the adviser to the Bachelor Project, nor the jury members nor the HEG.

“I attest that I have personally authored this work without using any sources other than those cited in the bibliography. Furthermore, I have sent the final version of this document for analysis by the plagiarism detection software stipulated by the school and by my adviser”.

Geneva, Friday 1st of June 2018

Romain GIMBLETT

Acknowledgements

This research paper was made possible with the guidance of Doctor Christophe Courbage. We would also like to thank Mr. Yves Keller, Mr. Antoine Spinelli, the person from UBS and the two people from HSBC for responding favourably to our interview requests and for taking the time to answer our questions.

Executive Summary

Operational risks are inherent in all banking products, activities, processes and systems; and must be managed closely. The operational risk management process aims at protecting the firm of potential losses but also at increasing the economic value of the entity. There are 6 main steps in a risk management process: identification, assessment, measurement, control and mitigation, monitoring, and creation of a continuity plan.

With the development of digital technologies, also called digitalization, customers are more demanding than ever in terms of level of service offered by their bank. This will force banking entities to rethink their business models, processes and systems. Therefore, the operational risks and the operational risk management process will be impacted by these modifications. This paper focuses on this change and aims at analysing how digitalization will affect operational risks and the operational risk management process in the Swiss banking industry.

The results of this study are based on existing research papers, qualitative interviews, and surveys. We interviewed 4 different banks in the Swiss financial sector to understand the point of view and opinion of people being closely involved with operational risk management. The outcome of these interviews is satisfying as opinions differ on certain points which made the analysis interesting. It appears that the impact of digitalization will be moderate. We should not see any new risks operational risks arise in the future. The most probable scenario is that we will observe a change in the impact or probability of occurrence of certain risks. We can also say that the main risks currently linked to digitalization are the cyber risk, model risk and contagion risk. In terms of the digitalization of the operational risk management process, this change should be positive for the human beings and the efficiency of the operational risk management teams. Indeed, we found that automated systems and processes will assist the human beings, but it should not replace them. Digitalization will play a key role in the upstream part of the process. This will guarantee an improved efficiency in terms of risk mitigation and a reduction in the underlying potential loss. We are strongly convinced that the profile of an employee working in the risk management department will change. It may be more focused on analytical skills and data science.

It will be interesting to see in five to ten years how the operational risks and the operational risk management process will actually be impacted.

Table of contents

Operational risk management in the digital era in the Swiss banking industry ... 1
Declaration ... i
Acknowledgements ... ii
Executive Summary ... iii
List of Figures ... vii
1. Introduction ... 1
1.1 Research question and statement of problem ... 1
1.2 Literature review ... 2
1.3 Research objectives ... 3
2. Theoretical foundations ... 4
2.1 Importance of risk management ... 4
2.1.1 The risk management process ... 5
2.2 Principles of the Sound Management of Operational Risk ... 6
2.2.1 The 11 fundamental principles of operational risk management established by the BCBS ... 7
2.3 FINMA requirements for operational risks at banks ... 8
2.3.1 The capital adequacy requirements ... 9
2.3.2 The qualitative requirements on handling operations ... 10
3. Analysis ... 13
3.1 Operational risks in the banking industry ... 13
3.1.1 The 4 sources of operational risk ... 13
3.1.2 The main operational risks ... 14
3.1.3 The management of operational risks ... 16
3.2 Digitalization of operational risk management ... 20
3.2.1 The impact of digitalization on operational risks ... 20
3.2.2 The seven key points to digitalize the risk management process ... 22
3.3 Insights from the industry ... 27
3.3.1 The methodology ... 27
3.3.2 The main sources of operational risks ... 27
3.3.3 The effect of digitalization on the operational risk management process ... 29
3.3.4 The evolution of the FINMA and Basel Committee Principles with the development of digitalization ... 31
3.3.5 The key points to digitalize successfully the operational risk management process ... 32
3.3.6 The impact of digitalization on the role of the human being in the operational risk management process ... 33
3.3.7 The new operational risks brought by the digitalization ... 34
4. Discussion ... 36
5. Conclusion ... 39
Bibliography ... 40

Appendix 1: 11 Principles for the sound operational risk management by the BCBS 43
Appendix 2: Art. 92, 93 and 94 Capital Adequacy Ordinance (CAO) 45
Appendix 3: Business lines allocation for the Standard Approach (SA, Art. 93 CAO) 46
Appendix 4: Illustrative key risk indicators 47
Appendix 5: Interview with Antoine Spinelli (BIC-BRED Suisse SA) 48
Appendix 6: Interview with Yves Keller (GS Banque) 51
Appendix 7: Survey – Yves Keller GS Banque 56
Appendix 8: Interview with a person from UBS Switzerland 59
Appendix 9: Survey – A person from UBS Switzerland 64
Appendix 10: Interview with 2 people from HSBC Switzerland 67
Appendix 11: Survey – 2 people from HSBC Switzerland 72

List of Figures

Figure 1: The 3 steps of the risk management process 5

Figure 2: Risk management strategies 6

Figure 3: Operational risk identification process 16

Figure 4: Model representation 21

Figure 5: The seven building blocks 22

Figure 6: The future impact of digitalization on the risk management process 22

Figure 7: Rating of the probable modification of the FINMA & BCBS Principles due to digitalization 30

Figure 8: Rating of the impact of digitalization on the role of human beings in the operational risk management process 32

Figure 9: Rating of the future impact of digitalization on operational risks 34

1. Introduction

1.1 Research question and statement of problem

This report analyses and attempts to answer the following question: How will digitalization affect operational risks and the management of such risks in the Swiss banking industry?

Nowadays, most of banks offer e-banking services where customers can access their account, pay bills and transfer funds. This is convenient but still limited as technology allows us to do much more such as taking out loans online. With the emergence of digitalization and the evolution of the society and technology in general, customers are demanding ever higher levels of service, value and trust.

Digitalization will force banks to rethink their business models and to deal with new operational risks. An important condition for an entity to be successful and to survive in the digital era is to manage risks at the perfection. Indeed, risk management allows to set pre-loss objectives such as minimizing the cost of risk and to set post-loss objectives that may avoid any business disruption, ensure a stable income or the survival of the firm.[1] It is relevant to focus on operational risks as they arise in almost all departments of the bank. Therefore, it is interesting to analyse how the operational risk management process of banks and the operational risks themselves will be affected by the development of digital technologies.

In order to avoid any confusion, we use "operational risk" as defined in Basel III[2]: "The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events. Strategic and reputational risk is not included in this definition […]."[3] In addition to this, we use "digitalization" as defined by Gartner Glossary: "Digitalization is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities […]."[4]

---

1 COURBAGE, C. (2017). [PDF] *The nature of risk and its treatment*

2 The Bank for International Settlements defines Basel III as an internationally agreed set of measures developed by the Basel Committee on Banking Supervision in response to the financial crisis of 2007-09. The measures aim to strengthen the regulation, supervision and risk management of banks.

3 BASEL COMMITTEE ON BANKING SUPERVISION. (2001). [PDF] *Consultative Document - Operational Risk*, p.2.

4 GARTNER IT GLOSSARY. (2018). *Digitalization - Gartner IT Glossary*. [online]

1.2 Literature review

On the one hand, the development of technologies has become deeply integrated in banking strategy and will take an even bigger importance in the near future. Indeed, the significant advantages of digitalization, with respect to customer experience, revenue, and cost, have become increasingly compelling for banks.[5]

On the other hand, the emergence of digitalization will force banks to rethink their business models and to deal with new operational risks (Chishti et al. 2016: 248-252).[6] Moreover, due to the evolution of technology and the high expectations of the society, customers are demanding ever higher levels of services, value and trust.[7]

Today, digital technology represents a great opportunity but also a threat to banks. One of these threats is the increase and development of operational risks. Deloitte's report "Navigating the year ahead – 2018 Banking regulatory outlook" addresses how digitalization will affect the business models of banks, however, it does not analyse how it will impact specifically operational risks and how entities will address these risks.[8]

PwC's research paper "Retail banking 2020: Evolution or Revolution" analyses what will be the impact of global macro-trends on retail banking and what will be the top 6 priorities for 2020 according to them. This study shows that 64% of executives are aware of the importance of proactively managing risks, including risks linked to digitalization, and that it is the biggest priority. However, only 22% of executives consider themselves really prepared. Therefore, there is a gap between awareness and preparedness.[9]

Sources that we have read focus a lot on what the experience for the customer will be like and how the business models of banks will evolve in the future. They don't focus on operational risk management as such and this is where we want to add value. Our aim is to introduce new information to future readers by tackling this gap and by analysing the impact of digitalization on operational risks and on the operational risk management processes in the Swiss banking industry.

---

5 GANGULY, S. et al. (2017). *Digital risk: Transforming risk management for the 2020s*. [PDF] McKinsey & Company

6 CHISHTI, S. and BARBERIS, J. (2016). *The fintech book*.

7 PILCHER, J. (2017). *Retail Banking 2020: Evolution or Revolution?* [online] The Financial Brand.

8 BALACHANDER, B. et al. (2017). *Navigating the year ahead 2018 banking regulatory outlook*. [PDF] United States: Deloitte.

9 PWC. (2016). [PDF]. *Retail Banking 2020: Evolution or Revolution*?

1.3 Research objectives

In order to answer our research question, we start by providing information related to the importance of risk management in the banking environment. We then detail the principles of operational risk management established by the Basel Committee on Banking Supervision as well as the requirements for operational risks at banks put in place by the FINMA. The latter give qualitative and quantitative requirements for the operational risk management process.

Secondly, we focus on the operational risks within the banking industry. We begin with a detailed review of the four sources of operational risks. We then approach the main operational risks faced by a bank (such as fraud or cyber-attacks) and the processes used to manage these risks.

Thirdly, we tackle the digitalization of operational risk management in two steps. We begin by analysing the impact of digitalization on operational risk and we develop seven key points to digitalize effectively the operational risk management process within a bank. In the second step, we use the data collected in our interviews to put into perspective what we could find in the literature. The purpose here is to have insights from different people in the Swiss financial industry to compare their point of views regarding the impact of digitalization on operational risks and on the operational risk management process. We had the opportunity to interview Mr. Antoine Spinelli, Chief Risk Officer at BIC-BRED (Suisse) SA; Mr. Yves Keller, Chief Financial Officer / Chief Risk Officer at GS Banque; a person working at UBS; and two people working at HSBC. It is interesting to put in comparison the different opinions from these professionals as well as the information collected during these interviews.

We conclude by summarizing the main findings of our analysis and by giving our recommendations.

2. Theoretical foundations

2.1 Importance of risk management

Operational risks are present in all banking products, activities, processes and systems; and must be managed closely. Risk management is a process that identifies pure risks faced by an entity and measures them. It then selects the best strategies to treat them effectively. In this paper, we focus solely on pure risks which only involve loss or no loss such as in the case of a computer hacking.[10] Therefore, we do not consider a pure Enterprise Risk Management (ERM) approach.[11] Risk management has purposes before and after the occurrence of a loss. Pre-loss objectives can be to minimize the cost of risk or to mitigate the anxiety of the employees. Post-loss objectives might be to ensure the continuity of the operations, the stability of the income or the survival of the entity.[12]

The objective of risk management is not only to protect the firm but also to increase the economic value of the entity which is defined as the present discounted value of the expected net cash flows in the future.[13] Risk management increases the net cash flow by decreasing the chance of having to raise new funds after a loss occurs, it reduces the chance of financial distress and cuts down tax payments by lessening the volatility of the cash flow. Risk management lowers the discount rate by reducing the cash flow volatility which in the end increases the entity's value. This is explained by the fact that there is a positive correlation between the volatility, the return expected by the owner and the discount rate.[14]

10 COURBAGE, C. (2017). [PDF] *Introduction to risk management*.

11 An ERM is a comprehensive risk management program that takes into account all the risks faced by an organization. (COURBAGE, C. (2017). [PDF] *Enterprise Risk Management (ERM)*)

12 COURBAGE, C. (2017). [PDF] *The nature of risk and its treatment*.

13 The formula used to compute the value create is: $Value = \sum_{t=1}^{\infty} \frac{Exp.\ net\ cash\ flow\ in\ \ year\ t}{(1+r)^t}$

14 COURBAGE, C. (2017). [PDF] *Introduction to risk management*.

2.1.1 The risk management process[15]

The risk management process usually includes the following 3 steps (Figure 1):

Figure 1: The 3 steps of the risk management process

Source: COURBAGE, C. (2017). [PDF] *Introduction to risk management*.

Risk analysis allows the firm to identify and classify the risks in order to prioritize them. The identification has for objective to review and list all the loss exposures. This can be done using several methods such as questionnaires, checklists or financial statements. The assessment and classification can be done using both qualitative and quantitative techniques (i.e. the Expected Value, the Value at Risk etc.). We will not go too much in depth regarding these techniques as the purpose is to understand the overall process of risk management.

Once the first step stated above has been achieved, several strategies may be put in place to manage risks. These strategies are divided into two distinct categories: “Risk control” and “Risk financing” (Figure 2). Risk control refers to actions that reduce the frequency or severity of a loss. These techniques are: “loss prevention”, “loss reduction” and “avoidance”. Loss prevention regroups activities aiming at reducing the probability of a loss (i.e. vaccines to reduce the probability of getting ill). Loss reduction regroups activities aiming at reducing the severity of a loss (i.e. water sprinklers spread out in a building to reduce the severity of a fire). Avoidance regroups activities aiming at eliminating the source of the risk by not undertaking the task (this is not always feasible). Risk financing refers to strategies that provide for the financing of losses after their occurrence. These strategies are: “retention” and “risk transfer”. Retention signifies using internal resources to finance the loss. Risk transfer signifies using external resources for the financing of the loss using for example insurance, contractual risk transfer or hedging.

[15] COURBAGE, C. (2017). [PDF] *Introduction to risk management*.

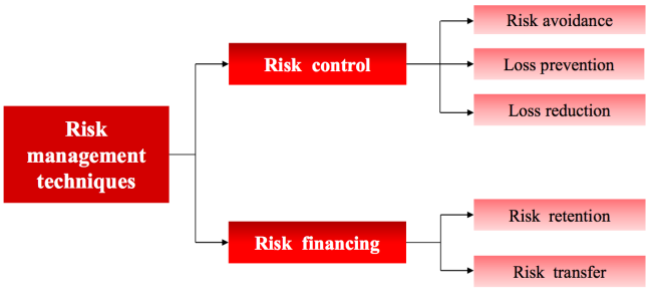


Figure 2: Risk management strategies

Source: COURBAGE, C. (2017). [PDF] *Introduction to risk management*.

A risk management process implementation begins with a risk management policy statement which summarizes the entity's objectives and policies, educates C-level executives and gives the authority needed to the risk manager. A rigorous intradepartmental cooperation is extremely important to ensure a global coverage of the firm. Finally, the risk management process and its underlying strategies must be reviewed on a periodic basis and constantly revaluated to determine if the objectives are being reached or if corrective measures must be put in place.

2.2 Principles of the Sound Management of Operational Risk

The Basel Committee on Banking Supervision[16] (BCBS) established a blueprint of principles for the banking industry called "Principles of Sound Management of Operational Risk". This document is part of the second pillar[17] of Basel III which is:

> *"an internationally agreed set of measures developed by the Basel Committee on Banking Supervision in response to the financial crisis of 2007-09. The measures aim to strengthen the regulation, supervision and risk management of banks. Like all Basel Committee standards, Basel III standards are minimum requirements which apply to internationally active banks. Members are committed to implementing and applying standards in their jurisdictions within the time frame established by the Committee." (Bank for International Settlements - Basel III: international regulatory framework for banks)*[18]

16 According to its own website: The Basel Committee on Banking Supervision (BCBS) is the primary global standard setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability. (*BIS.ORG. (2018). Basel Committee on Banking Supervision reforms - Basel III. [online]*)

17 There are 3 pillars, the first one concerns capital, risk coverage and containing leverage; the second pillar concerns risk management and supervision and the third pillar concerns market discipline. (*BIS.ORG. (2018). Basel Committee on Banking Supervision reforms - Basel III. [online]*)

18 BANK FOR INTERNATIONAL SETTLEMENTS. (2018). *Basel III: international regulatory framework for banks*. [online]

This second pillar addresses risk management and supervision.[19] The Basel committee states that the eleven principles presented under the next section (2.2.1) establish sound practices applicable to all banks and are to be interpreted as recommendations and not as a strict regulation. When implementing these principles, a bank must take into account the nature, the size, the complexity and the risk profile of its activities.[20] It is worth noting that as Basel I and II, Basel III is not legally binding in any jurisdiction but is rather a general basis for national law-making.[21] This explains why the FINMA's principles from the Circular 2008/21 presented under the section 2.3, which are associated to a legislation in Switzerland, are based on the BCBS's principles.

As a general notice, the senior management of a bank should ensure that the risk management framework's policies, processes and systems remain sufficiently sturdy; as the business environment is in a permanent change and operational risks are in a constant evolution.[22]

2.2.1 The 11 fundamental principles of operational risk management established by the BCBS[23]

The eleven principles of sound operational risk management cover corporate governance, the risk management environment and the role of disclosure. These principles published in 2011 have been elaborated after thorough discussions between supervisors and the industry since 2003. We can link these principles to each step of the risk management process detailed under point 2.1.1. The complete list can be found under Appendix 1.

Firstly, principles 1, 2 and 11, talking about the management culture, the general risk management framework and the public disclosures, are more of general terms at the macro level of the entity. Therefore, we will not detail them.

Secondly, principle 6 and 7 are related to the first step of the risk management process, which is the risk analysis. The senior management should guarantee a proper identification and assessment of the operational risks present in all material products,

19 BIS.ORG. (2018). *Basel Committee on Banking Supervision reforms - Basel III*. [online]

20 BANK FOR INTERNATIONAL SETTLEMENTS. (2011). [PDF] *Principles for the Sound Management of Operational Risk*, p.2.

21 SPINELLI, A. (2017). [PDF] *Risk Management for Banks, Regulatory implications*.

22 BANK FOR INTERNATIONAL SETTLEMENTS. (2011). [PDF] *Principles for the Sound Management of Operational Risk*, p.5.

23 BANK FOR INTERNATIONAL SETTLEMENTS. (2011). [PDF] *Principles for the Sound Management of Operational Risk*, p.1, 5-6.

activities, processes and systems to make sure that risks are well understood. Moreover, they should make sure that there is an approval procedure for all new products, activities, processes and systems so that operational risks are fully assessed.

Thirdly, principles 9 and 10 relate to the second step of the risk management process which is the risk management strategies. Indeed, banks should have a strong risk control environment which mitigates or avoids risks. Moreover, they should also have reliable resiliency and continuity plans to guarantee ongoing operations in case of a severe business disruption.

Finally, principles 3, 4, 5 and 8 relate to the third step of the process which is the implementation and monitoring. The board of directors should establish, approve and periodically review the risk management framework. In addition to this, it should approve and review a risk appetite and tolerance statement for operational risks according to the nature, types and levels of operational risks that the entity is comfortable with. The senior management has the responsibility of constantly implementing and maintaining policies, processes and systems to manage operational risks throughout the bank. The management has also the responsibility to implement a process allowing a regular monitoring of operational risks and material exposures to losses.

2.3 FINMA requirements for operational risks at banks

The FINMA is the independent supervisory authority of financial markets in Switzerland. It is responsible for ensuring a good functioning of the market. It supervises banks, insurance companies, exchanges, securities dealers, collective investment schemes, and their asset managers and fund management companies.[24]

The FINMA established capital adequacy requirements and qualitative requirements for operational risks at banks. Capital adequacy requirements represent the minimum capital that a bank must have in relation to their risk bearing capacity. These were issued in the circular 2008/21. According to Art. 7 para 1.1 let. B of the Financial Market Supervisory Act (FINMASA), the circulars aim to guarantee that the authority implements financial-market legislation consistently and effectively. FINMA circulars do not require any legal basis. However, their content must be associated to an underlying legal provision.[25] The circular 2008/21 sets out the basic qualitative requirements for

[24] FINMA (2018). *FINMA - an independent supervisory authority*. [online] FINMA.

[25] FINMA (2018). *FINMA's supervisory practice*. [online] FINMA.

operational risk management as per Art. 12 BO (Banking Ordinance) and Art. 19-21 SESTO (Stock Exchange Ordinance). In addition to this, it sets out how to determine the capital requirements for operational risks according to three different approaches.[26]

We will present first briefly the capital adequacy requirements as well as the qualitative requirements in the following sub-section.

2.3.1 The capital adequacy requirements

The three different methods to determine the capital requirements are the following: The Basic Indicator Approach (BIA), The Standard Approach (SA) and the Institution-Specific Approaches or Advanced Measurement Approach (AMA) which requires an authorisation by the FINMA. They are all detailed in the Capital Adequacy Ordinance (CAO) under Art. 92, 93 and 94 (Appendix 2). We will present the three methods below, however, we will not go too much into details as this is not the main focus of this thesis.[27]

The Basic Indicator Approach (BIA) has two main steps. Firstly, you have to compute the earning indicator for year N by adding the following positions on the profit and loss (P&L) statement for year N: result from interest income, result from fee and commission income, result from trading income, income from equity shares that don't need to be consolidated and the income from real estate. You then have to establish the average earning indicator on three previous years multiply it by 15% in order to obtain the minimum capital requirements for operational risks. [28]

The Standard Approach (SA) divides banking activities into eight business lines: corporate finance, trading and sales, retail banking, commercial banking, payment and settlement operations, custodial and fiduciary transactions, institutional asset management and retail brokerage. In each line, the gross income is used to represent the scale of business operations and thus, the probable exposure in terms of operational risk. The income in each line is multiplied by a percentage (ß) which is assigned to each one of them (Cf. table in Appendix 3). ß is a fixed value and is identical for all banks. Finally, the total capital is determined by summing all business lines within a year on the three previous years and computing the global average. When calculating the average, any negative summands must be set to zero according to Art. 93(1) CAO.[29]

---

26 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.5.

27 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.5-13.

28 SPINELLI, A. (2017). [PDF] *Risk Management for Banks, Regulatory implications*

29 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.7.

Finally, the Advanced Measurement Approach (AMA) allows banks to quantify capital requirements for operational risks according to their own method elaborated in-house. This gives greater flexibility to the entity as it can tailor its approach based on its business model and strategy. Applying to an AMA requires the authorisation of the FINMA, moreover, banks must respect certain requirements to undertake such an approach. Before giving the final approval, the FINMA may ask firms to run the different calculations based on their in-house model approach in order to test and compare the results for a maximum period of two years.[30]

2.3.2 The qualitative requirements on handling operations [31]

The following qualitative requirements are based on the principles of the Sound Management of Operational Risks issued by the BCBS that were presented previously and must be considered as a regulation in Switzerland. They are legally binding.

Principle 1: Operational risks should be categorized in a consistent way. This categorization should include an evaluation of the firm's inherent and residual risks. Such risks can be classified following two dimensions; "likelihood of occurrence" and "loss severity".

This principle fits perfectly in the spectrum of the first step of the risk management process "identification and assessment".

Principle 2: An adequate risk identification process, which is the support for the mitigation and the monitoring of operational risks, should take into consideration both internal and external parameters.

Indeed, operational risks can occur due to a mistake made by an employee as well as due to an external source.

Principle 3: An internal reporting on operational risks should use financial, operational and compliance inputs in addition to important external risk-relevant data on events and conditions.

This joins principle 6 of the BCBS which refers to the risk analysis step of the risk management process.

30 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.8.

31 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.15-19.

Principle 4: An IT risk management procedure based on the firm's information technology (IT) strategy and risk appetite should be developed by the executive management. It must take into consideration the internationally recognized standards. The IT risk management procedure should undertake the following functions:

- Assess what are the most important components of the network infrastructure;
- Define explicitly the roles, duties and responsibilities concerning critical applications in addition to IT infrastructure;
- Establish a systematic process to identify and assess IT risks;
- Train employees to enhance their awareness with respect to IT risks and how to mitigate them.

Secondly, the executives should put in place a cyber risk management process. It should undertake the following functions:

- Identification of potential threats coming from the internet or other similar networks affecting the integrity, availability and confidentiality of the IT infrastructures and disrupt business operations;
- Mitigation of the risk by protecting business processes and IT infrastructures from cyber-attacks;
- Prompt identification and recording of cyber-attacks with the use of specific processes and software;
- Rapid reaction to cyber-attacks with precise and targeted measures;
- Guarantee a prompt return to normal in case of business disruption.

These functions shall be tested frequently by the use of vulnerability and penetration tests in order to protect the IT infrastructure from cyber-attacks. These tests must be performed by qualified employees.

This principle is very important for this paper as it focuses on a specific type of operational risks that is and will most probably be affected by digitalization.

Principle 5: Business continuity plans must be put in place in order to guarantee the continuity of operations and limitation of potential damage in case of a major business disruption.

Principle 6: Banks should put in place a process ensuring the operating continuity of key functions.

Principle 7: If the entity undertakes operations abroad, it can face risks linked to the application of foreign legislations (tax laws, criminal laws, etc.). They must be documented, mitigated and controlled.

The presentation of the above principles set by the BCBS and the FINMA give us a good overview on what is expected from banks in terms of operational risk management. We can see that except from principle 9 (BCBS) and principle 4 (FINMA), none of the above tackle digital tools, such as Blockchain, and the operational risks linked to them. It will be interesting to see if the Principles remain broad in the future or if they target specific technologies.

Now that we have seen the operational risk management process, the following section will focus on the operational risks themselves.

3. Analysis

3.1 Operational risks in the banking industry

3.1.1 The 4 sources of operational risk

Operational risks may occur in any business area and affect the business process. Losses due to operational risks incidents are more important in areas such as system security, system failure, utility services and outsourcing of services. Keeping in mind the definition of the Basel Committee on operational risks, it is important to understand that they may occur from four different sources: people, processes, systems and external events.[32]

Operational risks related to personnel arise due to lack of knowledge regarding the procedures, doubtful staff at sensitive operational areas, absence of business ethics, compliant management towards corruption and poor supervision by the senior managers. Examples of such events may be act of fraud or registration of illegal transactions.[33]

Operational risks related to processes arise from the fact that banks have installed computer systems for cost optimization purposes. These systems process business transactions and concurrently capture and store all the transactions-related data. The assembly of the transaction processing function (for delivery of customer service) and the data classification storage function (to update the management information system) has increased the probability of error occurrence amid the processing stage. This generates defective information and messages that may cause financial losses of significant importance to banks. Examples of such events may be accounting errors, breach of procedures or inaccurate pricing of products and services.[34]

Operational risks related to systems arise from the fast-changing information technology system. Indeed, as a result of this massive evolution, banks must upgrade frequently the computer system and modify their software packages. Their IT systems are under harsh pressure and are very likely to be generating operational risks. Examples of such events

32 GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.390.

33 GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.390-391.

34 GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.391-392.

are failure of hardware and software systems, hacking or virus injection to the system or corrupting data processing.[35]

Operational risks arising from external events may lead to colossal financial losses causing a lengthened business disruption. Banks have absolutely no control over these events as they cannot predict the timing nor assess the intensity of the impact in advance. Such events may be robbery or failure of outsourced activities.[36]

3.1.2 The main operational risks

The FINMA has established a list of the main operational loss event categories that a bank may encounter. As we mentioned previously, all the operational risks are extremely important for a bank or any financial entity as they can have critical consequences.

We list the main operational loss event categories established by the FINMA below and we link them to the main source of risk as explained in section 3.1.1.

The first loss event category is “internal fraud”. This refers to losses that occur due to intended actions to defraud, swindle ownership or bypass regulations, legislations or business policies. This loss category involves at least one internal party. It is divided in two sub-categories which are “unauthorized activities” and “theft and fraud”. Unauthorized activities may be transactions that are not reported on purpose or entering financial positions wrongfully. Theft and fraud may be bribery or unauthorized access to accounts.[37] We may link this category to operational risks related to personnel.

The second loss event category is “external fraud”. This loss category regroups the exact same losses than the internal fraud category, however, it does not involve any internal party. It is divided in two sub-categories which are “theft and fraud” and “IT security”. The former regroups activities such as theft, robbery, etc. The later regroups activities such as damages caused by hacking, illegal data access leading to financial losses.[38] This category may be linked operational risks related to systems and to external events.

The third loss event category is “workplace”. It refers to losses that arise from the breach of labour, security or health laws and regulations. This includes all compensation payments. It is divided in three sub-categories which are “employees”, “occupational

35 GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.392.

36 GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.392-393.

37 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.23.

38 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.23.

safety" and "discrimination". Employees striking, breach of health and safety regulations and damages originating from discrimination are examples of activities that may incur losses to the firm.[39] This category may be linked primarily to operational risks related to personnel, however, we may also link it to risks related to processes.

The fourth loss event category is "clients, products and business practices". It refers to losses occurring because of an unintentional or negligent failure to fulfil a professional obligation towards clients, or from the design of a product. It is divided into 5 sub-categories which are "duties of suitability, disclosure and safe custody", "improper business or market practices", "problems with products", "client selection", "inappropriate business placement and credit exposure" and "advisory activities". Such activities may be: violation of banking secrecy, market manipulation, defective products, credit limit exceedances or a conflict in relation to the outcome of advisory services.[40] This loss event category may be linked to operational risks related to personnel and to processes.

The fifth loss event category is "damage to physical assets". This regroups losses that occur from damage to physical assets because of natural disasters or other external events. This category has a single sub-category named "catastrophes or other events". Examples are: natural disasters, vandalism or terrorism.[41] This category may be linked to operational risks related to external events.

The sixth loss event category is "business interruptions and system failures". This regroups losses occurring because of business disruptions or system breakdowns. It can be caused for example by a hardware, software or telecommunication failure.[42] This category may be linked to operational risks related to systems.

The seventh and final loss event category is "execution, delivery and process management". It regroups losses occurring as a result of inaccurate business processing or process management, from relations with business partners, vendors etc. This loss event is divided into 6 sub-categories. "Transaction capture, execution and maintenance" includes activities such as communication errors or missed deadlines. "Monitoring and reporting" includes activities such as inadequate reporting to external parties resulting in losses. "Client onboarding and documentation" includes activities such as non-compliance with internal and external regulations. "Client account management" includes

39 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.24.

40 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.25.

41 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.25.

42 KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.25.

activities such granting of non-authorized access to accounts. “Business partners” includes activities such as inadequate service or behaviour from a non-client business partner. “Vendor and suppliers” includes activities such as disputes with suppliers.[43] This loss event may be linked to operational risks related to personnel or external events.

3.1.3 The management of operational risks

This section details with a practical approach the 6 main steps of the operational risk management process which are, according to Ghosh: identification, assessment, measurement, control and mitigation, monitoring, and creation of a continuity plan.[44] In section 2.2.1 and 2.3.2 we saw the different operational risk management requirements imposed to banks from a legal and more theoretical standpoint.

The identification of operational risks should consider operational risks from all types of business activities, products and services throughout the bank. There are two distinct methods to identify these risks. Banks can follow a top-down or a bottom-up approach. Under the top-down approach, the bank’s activities are divided into business lines which may be corporate finance, trading and sales, retail banking, etc. Activity groups or product teams are then identified within each business line. After that, the products used in each line are separated and the risk events linked to each product are identified. Under the bottom-up approach, data on individual risk events are collected and are classified into broader event-type categories within each business line. Finally, risks are aggregated to get an overall picture of the operational risks faced by the bank.[45]

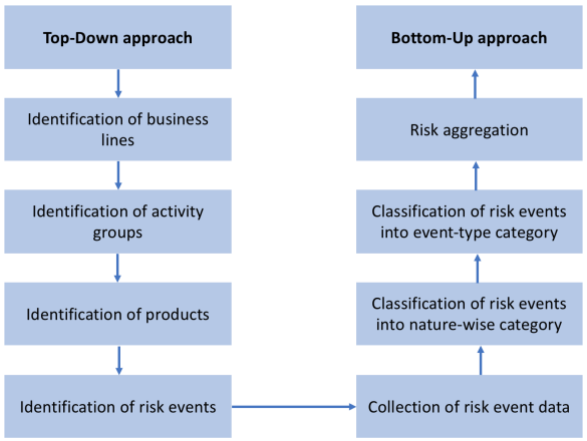


Figure 3: Operational risk identification process

Source: GHOSH, A. (2012). Managing risks in commercial and retail banking.

[43] KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*, pp.26.

[44] GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.409-411.

[45] GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.409-411.

The assessment of operational risks should be specific and tailored to each bank. It should keep all the activities, the business profile and the data availability in its spectrum. Unlike credit risk where the quantification is in potential credit loss, operational risks focuses its assessment of loss in relative terms such as “small, moderate, large and substantial”. Operational risk is more an issue of management rather than of measurement. Therefore, banks should assess enterprise-wide operational risk exposure, identify the high-loss areas and put in place a mitigating action. Three methods may be used to assess operational risks: control and risk self-assessment method, key risk indicator methods, and risk mapping method. We will only briefly explain each of these methods below as it is not the main point of focus of this paper.

Under the control and risk self-assessment technique, potential risk is assessed in terms of business processes and limits, skill requirement, and eventual threats and slippages. This allows to evaluate the strengths and weaknesses of the entire operational risk environment.

The second method is based on Key Risk Indicators (KRIs) which are statistics or metrics used to identify crucial areas where operational losses may occur. It highlights the activities and risk factors that have the biggest potential to inflict losses to the firm. KRIs give early warnings on people, processes and systems. They are based on three parameters: the business volume (i.e. volume of cash handled in a branch office), logistic support environment (i.e. ratio staff-workload) and discretionary power schedules (i.e. average number of excesses allowed). Examples of KRIs may be found in Appendix 4. Finally, the risk mapping method is used to identify the areas of weaknesses in order to prioritize corrective measures. Each bank should select its own parameters for risk mapping, collect the operational risk loss data from several business units and classify them accordingly.[46]

Operational risk measurement is used to know the size of potential losses in relation to business volume and income. It is used to assess the adequacy of capital versus expected and unexpected operational risk losses. Finally, it is used to evaluate the performance of business lines in terms of a loss to income ratio (operational loss vs. business line income). As mentioned previously, the Basel Committee has prescribed three methods to calculate the operational risk capital charges: The Basic Indicator Approach, the Standardized Approach and the Advanced Measurement Approach (AMA). The latter is the only method that indicates the methodology that allows the

[46] GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.414-421.

determination of potential operational risk loss. It is therefore an advantage to establish a methodology that follows the requirements of the AMA method to determine the operational risk regulatory capital. This method is able to generate two outputs: the expected loss and the unexpected loss from operational risk vulnerability. The New Basel Capital Accord specifies that a bank's internal measurement system must estimate the unexpected losses based on the use of internal and relevant external loss data, scenario analysis and bank-specific business environment and internal control factor. The crucial component of the operational risk measurement process is to estimate the potential loss based on the firm's own internal loss history. External data supplements the measurement process by capturing situations that internal data might not. It is available from peer banks, industry sources and other publicly available documents. Scenario analysis is used in sequence with the external loss data to assess a bank's exposure to high-severity events. This guides the bank on how to allocate its capital based on potential large operational risk losses.[47]

Banks should put in place an effective and reliable control mechanism supported by risk mitigation tools in order to minimize the impact of operational risks. The weaker the control framework, the greater the frequency and severity of loss events will be. It is important to keep in mind that a mitigation tool is not a substitute to a risk control. For example, if a bank takes an insurance for the cash handled at the counter, it does not mean that this bank can soften its controls regarding the respect of the procedures for handling cash in security. If this would be the case, the insurance could claim negligence in following the procedures against the bank. Insurance is a risk mitigation tool that is complementary to a risk control process and not a substitute. Such tools must be selected and put in place on a case-by-case basis in order to respond specifically to the risk exposure identified. More theoretically and as seen in point 2.1.1, a bank has three types of risk controls; loss prevention, loss reduction and avoidance. In terms of loss financing, it can either retain the loss and finance it with internal sources or it can be transferred by using an insurance for example.

Mitigation and control is a continuous process. The entity constantly has to review the operational risk causes and take the most appropriate remedial action. It can be to move employees around the firm in another department, upgrade IT systems or store sensitive data on a secured computer system to avoid any leakages. Finally, a bank should also assess constantly the capability of business line heads to identify and monitor low-

47 GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.421-424.

probability, high-severity operational risks and their ability to develop strategies to mitigate them.[48]

The monitoring phase aims at containing the frequency and the severity of loss events and to verify if the objectives put in place are being attained or if any corrective measures should be undertaken. The monitoring team uses resources such as past loss events, KRIs and reports transmitted by all the departments in the company. These reports are analysed by the bank in order to identify areas that must be monitored closely and more frequently. They must be comprehensive, contain the adequate data and be updated continuously to include new events and new scenarios taking place within the bank. Moreover, the cost of the risk management strategies should also be monitored, and adequate actions must be taken if the costs were to be too high. The monitoring function itself must be reviewed by designated officials to verify its effectiveness.[49]

Finally, following these measures, the risk management department has the responsibility to put in place a business continuity plan. This is a document that contains procedures for the restoration of near normal business operations in the event of a business disruption or failure taking place because of the occurrence of an operational risk event. Such plans deal with major emergencies that are on a very large scale and that arise from events that are not expected in the normal day-to-day business operations. The continuity plan targets at restoring the core activities of the bank on a priority basis. Payment and settlement, treasury, liquidity management, cash management, customer relations and risk management are the core activities of a bank.[50]

These six steps give us a good number of information on how operational risks are managed in the banking industry. However, the development of technology will impact operational risks and their management. We will see more about digitalization in the next section.

48 GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.430-431.

49 GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.429.

50 GHOSH, A. (2012). *Managing risks in commercial and retail banking*, pp.431-432.

3.2 Digitalization of operational risk management

3.2.1 The impact of digitalization on operational risks

Although the management of financial risks has strongly improved in the past 20 years, it is not the case for other risk types such as operational and compliance risks as they were not the costliest. The big increase in fines, damages and legal costs over the past 5 years has forced banks to give them more importance. Moreover, the use of digital channels causes existing risks to evolve and new risks to arise. Therefore, risk managers spend more time to identify, assess and mitigate them. Many of these risks are not truly "new risks", they are evolving and increasing as a result of structural changes due to the digitalization of business models and processes. However, crucial risks such as cyber risk, model risk and contagion risk have emerged and may be considered as the 3 main risks linked to digitalization nowadays.[51]

According to the Institute of Risk Management, cyber risk refers to any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its informational technology system.[52] This risk can be considered as the most important given the large amount of data that banks handle. A breach would be extremely costly. According to the Ponemon Institute[53], a cost analysis revealed that there is a positive correlation between the average total cost of data breach and the size of the incident. The average total cost ranged from $1.9 million for events with 10'000 implicated records or less, to $6.3 million for events with more than 50'000 implicated records.[54] Moreover, these attacks would not only disrupt the banks' operations, it will also risk all the confidential customer data stored by the entity. Given the current geopolitical context, it would not be surprising to see an increase in cyber security in the following years. This may not only happen at the institutional level but also across the industry in between banks. We might as well see a collaboration between the industry and the government to ensure a globally secured banking industry.[55]

Model risk is defined as the potential loss that a company may face due to the incorrect use or errors taking place in the development or the implementation of these models. A

51 HÄRLE, P. et al. (2015). *The future of bank risk management*. [PDF] McKinsey, pp.12-13.

52 THEIRM.ORG. (2018). *Cyber risk*. [online]

53 Ponemon Institute conducts independent research on privacy, data protection and information security policy. (Ponemon.org)

54 PONEMON. (2017). [PDF] *2017 cost of data breach study*, pp.6.

55 HÄRLE, P. et al. (2015). *The future of bank risk management*. [PDF] McKinsey, pp.13.

model is a quantitative method or system that exercises theories to process data into quantitative estimates used for decision making (Figure 4). Operational risk models such as a loss distribution approach model or an integration model may be used for regulatory, managerial and accounting purposes.[56] The number of models in large institutions rises by 10 to 25% per year and models become more complex, thus managing this risk closely is a must.[57]

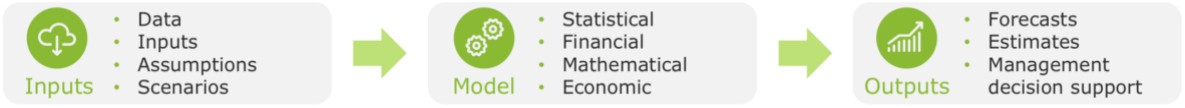


Figure 4: Model representation

Source: DELOITTE. (2017). [PDF] Model Risk Management - Driving the value in modelling.

For instance, a large US bank reported a loss of $6 billion which was partially due to a VaR[58] model risk. They had a lack of modelling experience, no back-testing had been done and there were operational problems in the model. In another case, an Asian bank lost $4 billion because its interest rate model was not accurate. They had not input the data correctly and there were significant errors in the model. These errors arise from various issues such as unreliable data and poor data quality, technical defects and implementation errors. Mitigation strategies focus on more rigorous and sophisticated model development using higher quality data, following a thorough validation process as well as monitoring and improving constantly the model.[59]

Contagion risk refers to the possibility that negative occurrences in one entity spreads to other entities and affects the financial markets. This could occur domestically but also across borders. It would ultimately cause losses to all or at least many actors of the industry. Digital and automated processes will act as a catalyst and increase the speed of the propagation. This risk is being monitored by regulators in order to avoid a general disruption in the financial system.[60] However, banks themselves must understand how they can be exposed and how they can mitigate it. Reducing this risk can cut down the banks total risk exposure and lower its capital requirements. The reason for this is that a

56 DELOITTE. (2017). [PDF] *Model Risk Management - Driving the value in modelling*, p.14-15.

57 MCKINSEY & COMPANY. (2018). *The evolution of model risk management*. [online]

58 VaR = Value at Risk

59 HÄRLE, P. et al. (2015). *The future of bank risk management*. [PDF] McKinsey, pp.13.

60 HARREIS, H. et al. (2017). *The future of risk management in the digital era*. [PDF] McKinsey & Company, pp.20.

banks' exposure to contagion risk is one of the main parameters for its classification as a global systemically important bank (G-SIB)[61] and for G-SIB capital surtax.[62]

The cyber, model and contagion risks are not necessarily "new", however, their growing importance and their impact has considerably changed. A robust and reliable risk management process is essential to guarantee an early identification and to put in place the best mitigation procedures.

3.2.2 The seven key points to digitalize the risk management process

To achieve a successful digitalization of the risk management process, banking institutions may rely on seven key points. While they do not need to master each one of them, banks will have to prioritize the points according to their strategy and develop the skills needed to reach their goals.

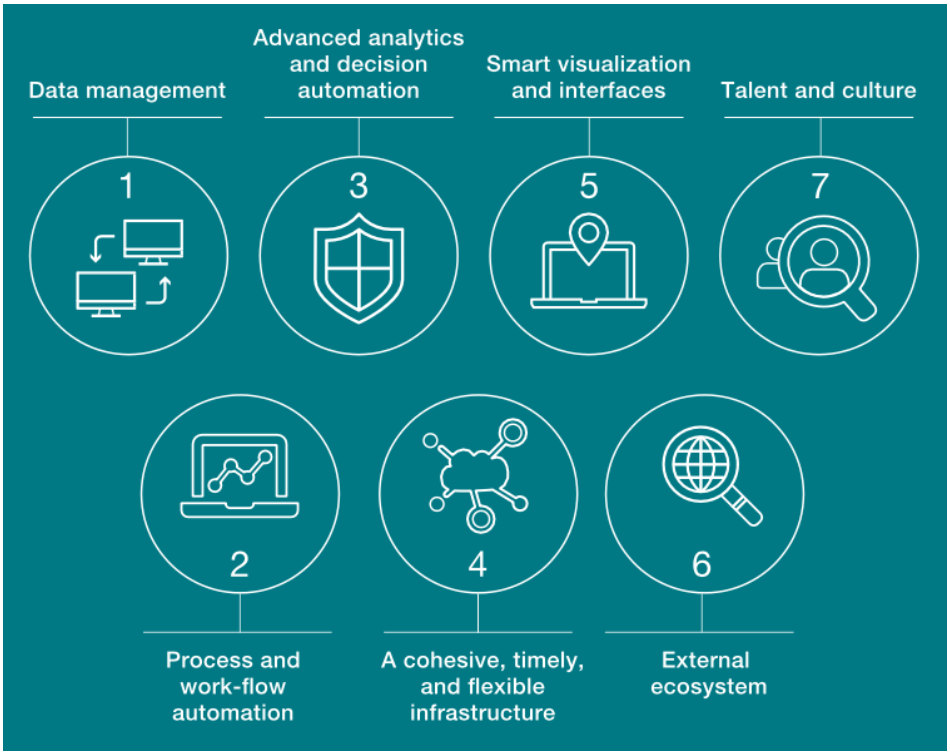


Figure 5: The seven key points

Source: HARREIS, H. et al. (2017). The future of risk management in the digital era. [PDF] McKinsey & Company.

61 A G-SIB is: "A financial institution whose distress or disorderly failure, because of its size, complexity and systemic interconnectedness, would cause significant disruption to the wider financial system and economic activity, and is therefore subject to additional capital buffers and increased supervisory scrutiny." (OSFI-BSIF.GC.CA. (2018). *Global Systemically Important Banks (G-SIBs).* [Online])

62 HÄRLE, P. et al. (2015). *The future of bank risk management*. [PDF] McKinsey, pp.13.

The data that banks generate and have under their control is represented by an increasing volume, velocity and variety. Indeed, the number of records stored and the pace at which this data is captured is rising. Moreover, banks are now able to work with new types of data such as chat transcripts or clickstreams. This signifies that the risk management process needs to have a sturdy approach and a well-defined process to handle and exploit the information. It is imperative that risk managers identify, assess and select the right type of data available to make timely and accurate decisions.[63] Furthermore, we know that the digitalization of internal processes will most probably cause new risks to arise. Therefore, banks will need to measure them, and it will create a need for new types of data.[64]

The use of an automated technological process reduces the need for manual intervention in key risk activities by reducing the number of inaccuracies and process times. When automating a process, it is important to redesign it from scratch to remove the unnecessary steps. We can think of two technologies in terms of RPA (robotic process automation) that operational risk managers may use. The optical character recognition would be able to read and understand documents digitally to extract relevant data. We can also think of the Blockchain technology which is already being implemented nowadays. Blockchain is a form of incorruptible decentralized distributed ledger listing transactions that is replicated, maintained and validated all at once by several stakeholders. This technology is extremely interesting for risk managers for three reasons. Firstly, it's a highly secure system due to its technological encryption and it supports smart contracts. Secondly, thanks to the high level of security, it is easier for risk managers to set automated controls and implement a default built in level of risk management directly within the Blockchain.[65] Finally, it will allow risk managers to reduce their costs thanks to automatic executions or reconciliations for example.[66]

It is worth noting that, like processes, decisions may be automated through the use of mathematical models. Advanced analytics can undertake more decision types, including predictions, the selection of best actions and the extraction of insights. Analytics use a wider array of algorithms which are now convenient thanks to the speed and power of

63 HARREIS, H. et al. (2017). *The future of risk management in the digital era*. [PDF] McKinsey & Company, pp.43.

64 HARREIS, H. et al. (2017). *The future of risk management in the digital era*. [PDF] McKinsey & Company, pp.43.

65 HARREIS, H. et al. (2017). *The future of risk management in the digital era*. [PDF] McKinsey & Company, pp.46-47.

66 BOUYALA, R. (2016). *La révolution FinTech*. RB Edition, p.103.

modern machines and the reliability of data. To undertake these tasks of automating decisions, risk managers will most probably need to hire data scientists and provide their teams with open-source software such as Python or R to code. These advanced analytics require a smooth integration with the other departments as it can bring benefits to risk management but also to other corporate units.[67]

The increasing volume of data has put banks' infrastructure under pressure due to the large number of sources of data (up to 1'000 different sources on average for one bank). Rearranging data infrastructure is a key objective for banks aiming at digitalizing their business model including their risk management process. Data lakes[68], an example of a flexible and scalable part of a hybrid data environment, can help risk management in different ways. They make real-time processing possible and allow new data processing techniques. They allow to store many different sorts of data at a low cost as you can keep them in the same store room.

Smart visualization and interfaces allow users to access information and data in an easier and more personalized way. Such technologies can be dashboards, interconnectivity between tools or augmented reality (AR). Risk managers are able to personalize the data and the information in order to improve their decision making. For example, the use of dashboards allows the user to have direct access to all the relevant information without having unnecessary data in front of his eyes. Moreover, each risk manager may have different needs in terms of data accessibility, therefore he will be able to customize its dashboard accordingly. These tools enable users to take more accurate and faster decisions. As incredible as it can be, AR can also be a great tool for risk managers. Indeed, we can think of AR glasses showing a world map. The user would move around the map by turning and tilting his head. As he passes on specific regions or countries, the risk data would pop up indicating precisely certain ratios or relevant information. Knowing that risk management in banks is generally conservative, these tools will help revolutionize and modernize the process.[69]

---

67 HARREIS, H. et al. (2017). *The future of risk management in the digital era*. [PDF] McKinsey & Company, pp.47-48.

68 "Data lakes promise rich analytical insights through faster data ingestion, but they are only a storage strategy." (HEUDECKER, N. et al. (2018). *Defining the Data Lake*. [online] Gartner.com.)

69 HARREIS, H. et al. (2017). *The future of risk management in the digital era*. [PDF] McKinsey & Company, pp.50-52.

Another important factor to digitalize risk management is the external ecosystem, more precisely, having access to external providers. FinTech[70] for example can help risk management deliver better solutions across various areas such as risk data support, technology development or operational loss risk mitigation. Collaboration between banks in risk and regulation issues are increasing. Risk managers use this to handle certain operational risks such as money laundering and operational loss risk mitigation, but it can be used for other risks such as third-party risk management. This reduces the amount of duplicative efforts as several banks may have access to this data stored on a shared platform. These utilities may be useful to counteract arising risks such as cyber risks and would allow banks to share analytics and data related to these in order to meet compliance surveillance requirements. However, banks should analyse closely the potential development in IT and cyber risks and the exposures that could arise with these partnerships. They should also verify if these alliances do not compromise any competitive advantage for the firm and it should cross-check these alliances with the local regulators. [71]

Last but not least, corporate culture and talent acquisition are necessary and key ingredients to a successful digitalization of the risk management process. It will require employees to have strong analytical proficiency. Data science and modelling expertise are considered as the most appropriate skills to digitalize risk management. The hiring method will have to change, and the recruiting timeline will have to be reduced. As data scientists are not in great numbers, banks should implement a training process that would allow current employees to improve in this sector. Furthermore, as data scientists may not necessarily be familiar with risk management in banks, a training program would help them get more comfortable with certain processes and have a better understanding of the risk management strategy.[72]

As a whole, banks will need to evaluate their strengths and weaknesses in each of the building blocks that we presented. They will then have to prioritize them according to

70 "Financial Technology, nowadays better known under the term 'fintech', describes a business that aims at providing financial services by making use of software and modern technology." (FINTECH WEEKLY DEFINITION. (2018). *FinTech - A definition by FinTech Weekly*. [online])

71 HARREIS, H. et al. (2017). *The future of risk management in the digital era*. [PDF] McKinsey & Company, pp.53-54.

72 HARREIS, H. et al. (2017). *The future of risk management in the digital era*. [PDF] McKinsey & Company, pp.54-56.

their importance regarding their corporate strategy and implement an action program to undertake the digitalization of their risk management process.

The next section will be focusing on the data collected on the field. It will allow us to have a better understanding of the opinion and point of view of people working in the Swiss banking industry and who are close to operational risks. Moreover, we will get a better understanding on what steps of the operational risk management process will be most influenced by digitalization.

3.3 Insights from the industry

The literature used for this paper has put in evidence questions that are interesting to ask to people closely involved with operational risk management in the Swiss banking industry. Indeed, it is relevant to go on the field and obtain information directly from professionals to base our analysis and draw our conclusions instead of simply relying on secondary data. Moreover, it is important to note that Switzerland is ranked 8th in the world by the International Institute for Management Development (IMD) in terms of world digital competitiveness in 2017.[73] Therefore, the point of view and the opinion from Swiss professionals on the digitalization of operational risks and the operational risk management process are expected to be very specific and in accordance with the capabilities of the industry.

3.3.1 The methodology

We have organized meetings with five different people from four different companies all from the Swiss banking industry. Mr. Antoine Spinelli from BIC-BRED (Suisse) SA, Mr. Yves Keller from GS Banque, a person from UBS Switzerland and two others from HSBC Switzerland have responded positively to our interview proposition. The people from UBS and HSBC asked us not to disclose their name, their field of work, nor their title. Therefore, we will name them "a person from UBS" and "the people from HSBC". The meetings lasted approximately 45 minutes, three of them took place in person and one of them over the phone. We asked the same six questions to our interviewees. After the meetings, each interviewee was asked to fill a survey allowing us to scale the answers and put them all into perspective. Unfortunately, only four out of five interviewees were able to return the survey completed. The data presented in the sub-sections 3.3.2 to 3.3.7 are the outcome of our interviews. All the interview transcripts as well as the surveys are included in their entirety in appendices 5 to 11.

3.3.2 The main sources of operational risks

Our interviewees have been unanimous when they were asked to determine what was the main source of operational risk in their company. All of them mentioned that the human error[74], such as a transaction booked wrongly, or a transaction not booked, was

[73] IMD BUSINESS SCHOOL. (2018). *World Digital Competitiveness Rankings 2017*. [online]

[74] It is a risk resulting from a mistake done by a human being and is to be classified in the source of risk resulting from personnel as seen in section 3.1.1.

the most important source of risk. Antoine Spinelli stated that it is important to have an efficient and reliable staff expertise to mitigate this risk. However, Yves Keller mentioned that, while an error made by a staff member is the operational risk that occurs the most often, the source of operational risk that leads to the biggest losses is the external events. On the one hand, banks have very robust and reliable internal systems and processes. There are controls that are put in place, that have been implemented and improved over time according to the person from UBS. Thanks to these, an operational risk resulting from a human mistake occurs but its impact in terms of financial loss is little. In addition to this, Mr. Keller said that for an internal fraud to take place, there needs to be a lot of collusion and this is difficult nowadays. On the other hand, banks may be exposed to external fraud because of corruption in a country for example. It is harder to control and mitigate, and the underlying financial loss may be much greater.

It is legitimate to ask ourselves if the operational losses due to human errors are forecasted. They are apparently usually so small that they aren't even forecasted. Limits are put in place to warn risk managers when and where they have to take action to mitigate a potential loss. According to Mr. Keller, the bank doesn't have an operational risk model that is going to determine the cost of capital. It is simply a percentage of the revenues from the last three years. What is interesting here is that we will be able to model this in the near future. For Yves Keller, the computation of the cost of capital must be much more granular than what it is today. It should take into account the financial loss history, the occurrence of losses and put them in perspective with the revenues. This could be done by building a model relying on algorithms that would gather the needed data and compute the underlying capital.

A very important parameter to consider as well when speaking about operational risks, is the continuous change. Indeed, new systems, processes and new products change the risk patterns of banks. Even if it is not recent, let's take the example of e-banking. It is nothing more than a client doing the operations by himself instead of going to a branch or sending a form to the bank. The transaction is the same, however it is done using a new channel. This channel represents a new risk according to the person from UBS. The client could enter wrong information or information that the system does not recognize. A risk of fraud is to be considered as well. You need to trust the log in system to make sure that it's Mr. XYZ that is on his account and not someone else. The development of digitalization might bring in some new risks in the future. This will be discussed in another sub-section further in this paper.

3.3.3 The effect of digitalization on the operational risk management process

Nowadays, there are already many automated tools that are used to monitor the operational risks according to Yves Keller. These tools allow banks to collect the information, to centralize them and to monitor them closely.

As operational risks are generally due to the human factor, digitalization has a special interest on the upstream part of the operational processes. Having processes and systems more automated will limit the risk of human errors. Antoine Spinelli states that a digitalized risk management process would aim at simplifying the manual tasks and assist the control environment. We can think of an automated operational risk control process relying on dashboards displaying live data. Yves Keller emphasizes that in order to be successful, the automated processes and systems must be built and designed extremely well from the very beginning. If this isn't respected, the residual risks would be important. The people from HSBC insist on the point that no matter how the operational risk management process is digitalized in the near future, a human being will still have a key role to play. Indeed, if the live data indicate an issue, a system won't be able to treat it by itself. A professional will have to take action and investigate. If the control environment has a weakness, risk managers will have to resolve it. This can't be done by an automated machine. However, they would find the digitalization useful in a specific area. They said that it is generally very difficult to identify the root cause of a problem because of the huge number of variables within a bank's processes. Therefore, it would be of great interest to have a unique system used by all the stakeholders involved in a workflow. It would have verification points to flow from one step to another by making sure that the data in the preceding step is correct. This system would have an assisting role towards the human being, it will by no means replace the intervention of a risk expert.

On another point of view, both Mr. Keller and Spinelli share the same future outlook on how the digitalization of the risk management process would be put into practice. An operational risk module will be implemented directly on the integrated banking software and will automatically seek for data. It is important that it is well connected to all the departments of the bank to be sure not to miss out on any potential operational risk. According to the hypotheses set at the implementation phase, the module will determine or identify abnormal transactions or transactions that shouldn't have been done. Risk managers will be notified immediately, and they will be able to take action very rapidly. The closer the action is to the operational risk event, the more efficient the response from

the risk managers will be and the more chances they will have to mitigate the loss. Antoine Spinelli mentioned that a digital risk management process doesn't necessarily need to go more in depth than a human. It will bring more completeness regarding the analysis of the transactions and this will result in more complete controls. Finally, the analysis of the deals won't be done using a sampling technique anymore. It is time consuming and not efficient. The process will look at the global pool of transactions made by the company and will pick all transactions that should be investigated.

A digitalized operational risk management process must be granular enough to spot the small details that may lead to a potential loss, while still being able to let the transactions flow through, said the person from UBS. For this, you need a margin of error that you are comfortable with. Digitalization means that you also have to be protective from the outer world on how you use the data and what type of data you use. It is critical to find the proper way to exploit the data at its maximum while making sure not to be hacked.

Assuming that banks digitalize their entire business models in the future, everything will go a lot faster. In the Blockchain for example, transactions are booked in a decentralized ledger where you can't amend the deal once it is registered. The time needed to settle a trade using the Ripple Blockchain for example is almost instant, whereas a bank settles a trade in three to five days actually.[75] This will increase the need in operational risk controls, according to the person from UBS, as you need to make sure that you don't miss out on something before it is too late. Yves Keller adds that if the transaction recorded on the Blockchain is done strictly between the beneficiary and the issuer, that no other intermediary is involved, there are no reasons to see any increase in the risk level.

The survey indicates that our candidates evaluate the future impact of digitalization on the risk management process as very important.

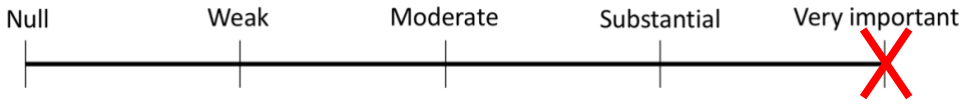


Figure 6: Rating of the future impact of digitalization on the risk management process

[75] RIPPLE. (2018). *Ripple - One Frictionless Experience To Send Money Globally | Ripple*. [online]

3.3.4 The evolution of the FINMA and Basel Committee Principles with the development of digitalization

These Principles are very broad and very generic stated Mr. Keller. There would be no need to make any changes, said Mr. Spinelli. The FINMA and BCBS Principles will have to change and they will need to adapt, replied the person from UBS, and the people from HSBC. These are very divergent opinions resulting from our interviews. It is important that these Principles must be applicable to all the banks in Switzerland. According to Antoine Spinelli, there are more than 250 banks from different sizes in the country. Therefore, these Principles must follow a ratio of proportionality and have as objective to set a regulatory framework for operational risk management in which banks can work. You cannot impose the same requirements to a Swiss bank having several offices around the globe than to a small Swiss bank operating only in its vicinity.

Mr. Keller thinks that these Principles will take the digital into account in the future, but this will depend on the speed of this evolution. They will most probably remain broad, however, if we see a certain technology that is used more than others (i.e. Blockchain), it may be integrated to a Principle. If we see a real change in processes, the FINMA and the BCBS will have to change their Principles, said the person from UBS. If we stop using credit cards for example and people only use tools like Twint to complete a payment, it will most probably be reflected in the Principles as the framework won't be the same anymore.

According to the person from UBS, regulations are delayed compared to where the industry is currently. Therefore, he sees a delay in the implementation of the technology and the creation of the underlying rules and regulations.

The survey indicates that our candidates evaluate a potential modification of the FINMA and Basel Committee Principles due to a digitalization of the operational risk management process as likely.

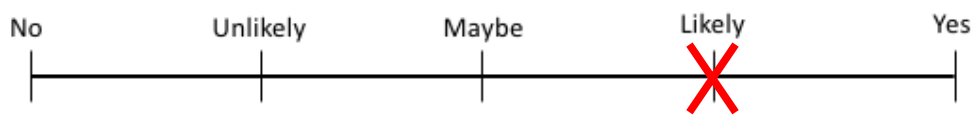


Figure 7: Rating of the probable modification of the FINMA & BCBS Principles due to digitalization

3.3.5 The key points to digitalize successfully the operational risk management process

The digitalization of the operational risk management process can be prioritized in many different ways. Banks can decide to focus at first on the corporate culture or they can modify their processes and systems while adapting the culture and the workforce around them.

Antoine Spinelli sees operational risk management as two distinct pieces. The first one is the regulation part and the second one is the operational part. The most important parameter to consider is that the digitalized operational risk management process manages the risks effectively while respecting the regulation. On the operational side, it has to assist the operational risk managers by collecting and bringing up to them key data and information to base their decisions and actions on. Yves Keller insists on the fact that the digitalized module of operational risk management must be well connected to the entire bank in order to guarantee its effectiveness. This digitalized process will allow risk managers to have a global overview of what is happening live within the bank. Mr. Keller adds that today, the operational risk is usually brought to light when the person that committed the error announces it. This is often too late as the loss already took place. The advantage of digitalizing the operational risk management process is to have a module that will detect the risk as upstream as possible. The people from HSBC mentioned that it was extremely difficult to have access to certain types of data when they had to make an analysis or solve an issue. On the one side, they think that a key step to digitalize the risk management process is to find a way to have access to any type of data when needed. In addition to this, it will be extremely important to guarantee the reliability and the quality of the data. On the other side, they affirm that before considering digitalizing the whole operational risk management process, it is important to improve the actual dashboards, ratios etc. According to the people from HSBC, there are many banks that are still at the stage of defining what metrics they would like to use in their dashboards. On that note, a very useful technology that they would be keen to implement would be a software on which all the people implied in the operational risk management, in the controls linked to these risks and in the testing of these controls can input their data and see the data of the others. This would allow a direct interaction between all the parties and a more efficient exchange of data and information.

To build a successful digitalized operational risk management process and a successful model, it is imperative for banks to make sure that the models, robots or any

programmable technologies are well coded from day one. Here again, the biggest source of risk is the human being, if the technology is not well built by the human, big risks and underlying losses could arise, said the person from UBS. It will be important to analyse Big Data in order to create a predictive model. This will allow the creation of trends, based on past data, and if the actual data collected by the model does not match the previous trends, it will trigger alerts. The risk managers will then know precisely where they need to put in place their controls to manage the operational risk effectively and efficiently. According to Mr. Spinelli, the quality and the reliability of the data is key. This is what is going to determine a good technological system to manage operational risks in a bank.

A new technology that would revolutionize the way operational risks are managed would be a model that could estimate whatever operational risk could potentially arise before the bank would even encounter it. This would be extremely powerful said the person from UBS. This is a long shot, but it would be a very new approach to operational risk management.

3.3.6 The impact of digitalization on the role of the human being in the operational risk management process

Nowadays, there are people gathering and analysing the data, that make the framework and that make the controls according to the person from UBS. No matter how technology improves and develops, the human being will still be needed in the future to analyse the situations from a global standpoint with a holistic view. The technology will give the data that needs to be analysed and interpreted by humans. They will have to put it into perspective with a situation said Yves Keller. For example, a transaction may seem abnormal, it may trigger an alert in the automatized system, however, as there is a special situation, it is good to let it flow through. The model might not be able to do such things, so the human has to do it. A big portion of the quantitative part may be digitalized; however, humans will be needed for the qualitative part of the operational risk management process. A real person will have to put the data in perspective with the risk appetite of the bank, the reality of the field and the needs of the bank according to the people from HSBC. Risk management is not binary, the human eye, the opinion of an expert will always be needed. We can certainly automatize KCI's, KRI's or KPI's[76] but when an alert is triggered, a human being needs to investigate what happened and if the issue is linked to a human, a process, a system or an external event. It is important to

[76] KCI = Key Control Indicator, KRI = Key Risk Indicator, and KPI = Key Performance Indicator

understand that the senior management of the bank is also expecting a real person to be in charge of certain risks, who masters the subject and who can bear the consequences stated the people from HSBC.

There will be less people doing what we call “data crunching”, which is basically the analysis of data. They will be replaced by machines that will mostly give quantitative information, but they might also give qualitative information to understand why and how something happened. The human will then have to investigate and put the information into perspective. The digital technology will have the role of an advisor but definitely not a role of decision making affirmed Antoine Spinelli. The regulators would not allow a machine to handle the risks by itself and make the decisions added the person from UBS and the people from HSBC. If something goes wrong, the human being is the only one liable at the end of the day. In the future, we might see more people building frameworks and models. These people will need to think for the automated programs as the technology can only do what you program it for. Artificial intelligence is way too futuristic said the person from UBS.

The survey indicates that our candidates evaluate the impact of digitalization on the role of human beings within the operational risk management process as substantial.

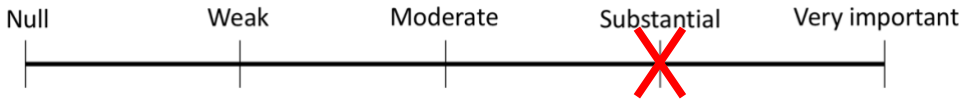


Figure 8: Rating of the impact of digitalization on the role of human beings in the operational risk management process

3.3.7 The new operational risks brought by the digitalization

All the operational risks exist already, and we shouldn’t really encounter new ones with the development of digitalization answered all of our interviewees. If a bank starts using a new technology, it doesn’t mean that it will necessarily increase the underlying risk. It depends on how the entity sees the risks, how it manages the risk and how it manages its data said Yves Keller. More than seeing changed or new operational risks, we will observe a change in the underlying controls stated the people from HSBC. In addition to this, they don’t think that the impact or the probability of occurrence of the contagion risk and the cyber risk will increase. Antoine Spinelli sees an increasing magnitude of the cyber risk which will require to put in place a control of the control system within the bank. Yves Keller thinks that if the industry is focusing mainly on digital processes, banks may

be more exposed than they are today, however, they will adapt their way of managing risks in accordance with the new practices. Overall, the impact of digitalization on operational risks won't be more important than what it is today, and the residual risk won't be greater.

Banking entities are interconnected and will probably be even more in the future with the development of technology, stated Antoine Spinelli. However, he adds that banks are not and will not be interconnected enough to see a global disruption of the banking industry in Switzerland. Mr. Spinelli, Mr. Keller and the person from UBS mention and emphasize that it will be important for banks to stay in their own environment, to develop their own models and technology in-house in order to avoid unnecessary risks. If every bank uses the same technology, it will be very easy for hackers to put the whole industry down. The contagion risk can be a great threat for the Swiss banking industry stated the person from UBS. However, he adds that big banks such as UBS will rely on their own model and own processes and won't rely on external systems. This will mitigate in some way the contagion risk. The people from HSBC also doubt that a single model can fit all the banks in Switzerland. They have to be tailor made to suit the precise needs of each entity.

What is interesting is that banks are actually aiming at centralizing their systems according to what the person of UBS has read in the press. This brings in a new risk in addition to the cyber risk. Indeed, if Swiss banks were to have a centralized system, there would be a physical risk. For example, if the entities had all their servers stored at one company's warehouse. If the building caught fire and burned, there wouldn't be one bank down, there would be all the banks having their servers in this warehouse that would be taken down. Therefore, risk managers will prioritize having their own infrastructure according to the person from UBS.

The survey indicates that our candidates evaluate the future impact of digitalization on the operational risks as moderate.

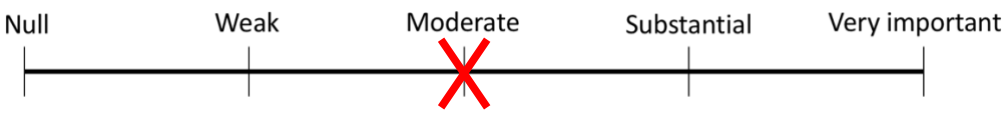


Figure 9: Rating of the future impact of digitalization on operational risks

The next section of this paper will be dedicated to a summary of our findings, the overall outcome and the conclusion of our analysis.

4. Discussion

This section summarizes the findings of our analysis and our point of view on the impact of digitalization on operational risks and the operational risk management process in the Swiss banking industry.

According to our interviews, the main source of operational risks is the human error. However, the external event is the source leading to the greatest losses. These types of risks are very hard to predict and to control for banks. The “continuous change” is not one of the four classical sources[77] of operational risks that we can find in the literature, however, we think that it has a big role to play. Indeed, in a constantly changing environment, banks might encounter changing operational risks. In order to mitigate these, we think that the entity must be very flexible and adapt rapidly its operational risk management process to avoid being exposed.[78]

Prior to meeting the five professionals for our interviews, and with the information found in the literature, we thought that the operational risks would change consequently in the near future with the development of digitalization. However, we can see that operational risks are not likely to change. Our interviewees are unanimous, all the operational risks exist, and we shouldn’t see new ones in the future. We personally think that if banks’ business models take a ninety-degrees turn and operations are done very differently in the future, banks might encounter new risks. Nonetheless, as our interviewees mentioned, this is not likely to occur. Regarding cyber risks and contagion risks, four of the five people we interviewed don’t expect any changes in terms of impact or probability of occurrence. We hold the view that if processes become digitalized to a certain extent, that banks become interconnected within the whole Swiss industry, these risks might see their impact increase. The probability of occurrence will depend mostly on the controls put in place by the banks and how they configure their information technology security. As we could find in the literature, we might see a collaboration between the industry and the government to ensure a globally secured banking industry.[79] In our opinion, this would allow to mitigate the contagion risk from an external point of view with a sort of an industry wide alliance. Finally, it will be important for banks to remain focused on their own internal development. It is recommended that they operate with models, processes

77 As seen in section 3.1.1.

78 See Appendices 5 to 11 with the transcript of the interviews

79 HÄRLE, P. et al. (2015). *The future of bank risk management*. [PDF] McKinsey, pp.13.

and systems built and designed in-house tailored to their specific needs and expectations.[80]

Concerning the impact of digitalization on the Principles of the FINMA and the Basel Committee on Banking Supervision (BCBS), the opinions of our interviewees were very different. We share the same point of view as Yves Keller. We believe that the Principles will remain broad as their role is to set a regulatory framework in which financial entities can work. Nonetheless, if we see a certain type of technology emerging and being used widely throughout the industry, it might be integrated directly into one or several Principles. What will be interesting to observe is how much time will be needed for the FINMA and the BCBS to amend their Principles. Indeed, according to the person from UBS, the Swiss regulation is delayed compared to where the industry currently is.[81]

Automated processes resulting from a development of digitalization will allow banks to limit human errors. We believe that three steps of the risk management process may be digitalised. The identification, the control and the monitoring of operational risks are tasks that may be handled by automated systems or processes in the future. If they are not entirely handled automatically, risk managers will be strongly assisted by technology in these various steps. The outcome of our analysis shows that digitalization will have a great importance on the upstream part of the operational risk management process. Indeed, as human error is the most important source of risks, a digitalized process will simplify the manual tasks and assist the human beings in their daily work. As humans will rely on the information and data brought up by the technology, the systems and processes must be built extremely well from the very beginning and use data that are reliable and of quality. The overall system must be well connected to all the departments of the bank to ensure a global coverage and to be sure not to miss any operational risk event. [82]

Our point of view concerning the role of technology in the operational risk management process has changed after having conducted our interviews. We initially thought that a digitalized operational risk management process would be able to manage up to a certain extent the risk exposures by itself. Of course, it was clear to us that humans were needed to configure the models and the systems, and to monitor them. However, our discussions with professionals gave us a whole other perspective. We now share a perspective close

80 See Appendices 5 to 11 with the transcript of the interviews

81 See Appendices 5 to 11 with the transcript of the interviews

82 See Appendices 5 to 11 with the transcript of the interviews

to what Yves Keller and Antoine Spinelli have demonstrated. An operational risk module will be implemented directly on the integrated banking software and will automatically seek for data within all the departments of the bank. This will guarantee an effective coverage and will assure managers not to miss any potential risk. This joins the bottom-up approach used in the identification of operational risks as we saw under point 3.1.3. which seems to be the most appropriate technique to use with a digitalized process. The true advantage of digitalizing the operational risk management process is to have a module that will detect the risk as upstream as possible. Risk managers would then be able to put in place a control and a loss mitigation procedure almost instantly and very close to the risk event.[83]

The development of digitalization in the process of managing operational risks won't threaten the role of human beings. We think that it will modify slightly its daily tasks, however, the human expertise will still have a big importance. A big part of the quantitative analysis will be digitalized but the qualitative part is very difficult to automate. A real person will have to put the data in perspective with the situation in which it was collected. The digital technology will have a role of assistance but not a role of decision making. If something goes wrong, the human is the only one to be liable at the end of the day. Moreover, industry regulators and banks' top executives feel more comfortable if a certain person is responsible to manage a specific risk rather than a machine.[84] This brings us to the point that a strong corporate culture focused on digitalisation and effective talent acquisitions are key ingredients to a successful digitalization of the operational risk management process. We believe that a risk manager will need to have a strong analytical proficiency in addition to having a modelling or data science background. If the employees recruited have less of a risk management background, we would recommend banks to set up a training program to familiarize the new comers with certain processes and develop their understanding of risk management.

83 See Appendices 5 to 11 with the transcript of the interviews

84 See Appendices 5 to 11 with the transcript of the interviews

5. Conclusion

In conclusion, the impact of digitalization on operational risks will be moderate. We shouldn't see any new risks arising. However, we will most probably see a change in the impact or in the probability of occurrence of known risks such as cyber or contagion risks. The impact of digitalization on the operational risk management process will be very important. Automated systems and processes will assist human being on a daily basis by covering the entire departments of the bank and will allow risk managers to take action much quicker than nowadays. The digitalization will play a key role on the upstream part of the process. It will guarantee a more effective mitigation of the potential loss underlying the risk. The human eye and expertise will remain an important part of the process. What will most likely change, according to us, is the profile of an employee working in the risk department. It will be more focused on analytical skills and data science background. We think that managers and executives must be cautious and must be not only aware of digitalization, but they should also be prepared for it. It will arrive extremely quickly and banks that don't catch the trend will most probably be left behind.

The impact of digitalization on operational risks and the operational risk management process may be interpreted in different ways as we saw during the interviews. It will be interesting to see, in five to ten years, what the noticeable changes are and how this key function of a bank will have evolved.

Bibliography

BALACHANDER, B. et al. (2017). *Navigating the year ahead 2018 banking regulatory outlook*. [PDF] United States: Deloitte. Available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-regulatory-banking-outlook-2018.pdf [Accessed 17 Mar. 2018].

BANK FOR INTERNATIONAL SETTLEMENTS. (2011). [PDF] *Principles for the Sound Management of Operational Risk*. Available at: https://www.bis.org/publ/bcbs195.pdf [Accessed 18 Mar. 2018].

BANK FOR INTERNATIONAL SETTLEMENTS. (2018). *Basel III: international regulatory framework for banks*. [online] Available at: https://www.bis.org/bcbs/basel3.htm [Accessed 18 Mar. 2018].

BASEL COMMITTEE ON BANKING SUPERVISION. (2001). [PDF] *Consultative Document - Operational Risk*. Available at: https://www.bis.org/publ/bcbsca07.pdf [Accessed 15 Mar. 2018].

BIS.ORG. (2018). *Basel Committee on Banking Supervision reforms - Basel III*. [online] Available at: https://www.bis.org/bcbs/basel3/b3summarytable.pdf [Accessed 26 Mar. 2018].

BOUYALA, R. (2016). *La révolution FinTech*. RB Edition.

CHISHTI, S. and BARBERIS, J. (2016). *The fintech book*. Chichester: Wiley.

COURBAGE, C. (2017). [PDF] *Enterprise Risk Management (ERM)*. Course slides: Course “International risk management”, Haute Ecole de Gestion de Genève, Semester fall 2017

COURBAGE, C. (2017). [PDF] *Introduction to risk management*. Course slides: Course “International risk management”, Haute Ecole de Gestion de Genève, Semester fall 2017

COURBAGE, C. (2017). [PDF] *The nature of risk and its treatment*. Course slides: Course “International risk management”, Haute Ecole de Gestion de Genève, Semester fall 2017

DELOITTE. (2017). [PDF] *Model Risk Management - Driving the value in modelling*. Available at: https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/risk/deloitte_model-risk-management_plaquette.pdf [Accessed 5 Apr. 2018].

FINMA (2018). *FINMA - an independent supervisory authority*. [online] FINMA. Available at: https://www.finma.ch/en/finma/finma-an-overview/ [Accessed 20 Mar. 2018].

FINMA (2018). *FINMA’s supervisory practice*. [online] FINMA. Available at: https://www.finma.ch/en/documentation/circulars/#Order=2 [Accessed 20 Mar. 2018].

FINTECH WEEKLY DEFINITION. (2018). *FinTech - A definition by FinTech Weekly*. [online] Available at: https://www.fintechweekly.com/fintech-definition [Accessed 20 May 2018].

GANGULY, S., HARREIS, H., MARGOLIS, B. AND ROWSHANKISH, K. (2017). *Digital risk: Transforming risk management for the 2020s*. [PDF] McKinsey & Company. Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Digital%20risk%20Transforming%20risk%20management%20for%20the%202020s/Digital-risk-Transforming-risk-management-for-the-2020s.ashx [Accessed 15 Mar. 2018].

GARTNER IT GLOSSARY. (2018). *Digitalization - Gartner IT Glossary*. [online] Available at: https://www.gartner.com/it-glossary/digitalization/ [Accessed 21 Mar. 2018].

GHOSH, A. (2012). *Managing risks in commercial and retail banking*. Singapore: John Wiley & Sons Singapore. ISBN: 9781118103531

HÄRLE, P. et al. (2015). *The future of bank risk management*. [PDF] McKinsey. Available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-bank-risk-management [Accessed 17 Apr. 2018].

HARREIS, H. et al. (2017). *The future of risk management in the digital era*. [PDF] McKinsey & Company. Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20future%20of%20risk%20management%20in%20the%20digital%20era/Future-of-risk-management-in-the-digital-era-IIF-and-McKinsey.ashx [Accessed 3 Apr. 2018].

HEUDECKER, N., BEYER, M. AND RANDALL, L. (2018). *Defining the Data Lake*. [online] Gartner.com. Available at: https://www.gartner.com/doc/3053217/defining-data-lake [Accessed 20 May 2018].

IMD BUSINESS SCHOOL. (2018). *World Digital Competitiveness Rankings 2017*. [online] Available at: https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2017/ [Accessed 20 May 2018].

KPMG. (2016). [PDF] *Circular 2008/21 operational risk – banks*. Available at: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/ch-finma-circular-2008-21-en.pdf [Accessed 20 Mar. 2018].

KPMG. (2017). [PDF] *Ordinance on Capital Adequacy and Risk Diversification for Banks and Securities Dealers*. Available at: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/ch-ordinance-concerning-capital-adequacy-en.pdf [Accessed 26 Mar. 2018].

MCKINSEY & COMPANY. (2018). *The evolution of model risk management*. [online] Available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-evolution-of-model-risk-management [Accessed 5 Apr. 2018].

MCKINSEY & COMPANY. (2018). *The future of risk management in the digital era*. [online] Available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-risk-management-in-the-digital-era [Accessed 11 Apr. 2018].

MCKINSEY. (2015). [PDF] *The future of bank risk management*. Available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-bank-risk-management [Accessed 17 Apr. 2018].

OSFI-BSIF.GC.CA. (2018). *Global Systemically Important Banks (G-SIBs).* [online] Available at: http://www.osfi-bsif.gc.ca/Eng/Docs/nr20171121_ig.pdf [Accessed 20 May 2018].

PILCHER, J. (2017). *Retail Banking 2020: Evolution or Revolution?* [online] The Financial Brand. Available at: https://thefinancialbrand.com/56988/retail-banking-strategy-2020/ [Accessed 15 Mar. 2018].

PONEMON. (2017). [PDF] *2017 cost of data breach study*, p.6. Available at: https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130wwen/security-ibm-security-services-se-research-report-sel03130wwen-20180122.pdf [Accessed 4 Apr. 2018].

PWC. (2016). [PDF]. *Retail Banking 2020: Evolution or Revolution*? Available at: https://www.pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf [Accessed 17 Mar. 2018].

RIPPLE. (2018). *Ripple - One Frictionless Experience To Send Money Globally* | *Ripple*. [online] Available at: https://ripple.com [Accessed 6 May 2018].

SPINELLI, A. (2017). [PDF] *Risk Management for Banks, Regulatory implications*. Presentation slides: Course “International risk management”, Haute Ecole de Gestion de Genève, Semester fall 2017

THEIRM.ORG. (2018). *Cyber risk*. [online] Available at: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/ [Accessed 4 Apr. 2018].

Appendix 1: 11 Principles for the sound operational risk management by the BCBS

Fundamental principles of operational risk management

Principle 1: The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management[9] should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture[10] exists throughout the whole organisation.

Principle 2: Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.

Governance[11]

The Board of Directors

Principle 3: The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

Principle 4: The board of directors should approve and review a risk appetite and tolerance statement[12] for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

---

[9] This paper refers to a management structure composed of a board of directors and senior management. The Committee is aware that there are significant differences in legislative and regulatory frameworks across countries as regards the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) so as to ensure that the latter fulfils its tasks. For this reason, in some cases, it is known as a supervisory board. This means that the board has no executive functions. In other countries, the board has a broader competence in that it lays down the general framework for the management of the bank. Owing to these differences, the terms "board of directors" and "senior management" are used in this paper not to identify legal constructs but rather to label two decision-making functions within a bank.

[10] Internal operational risk culture is taken to mean the combined set of individual and corporate values, attitudes, competencies and behaviour that determine a firm's commitment to and style of operational risk management.

[11] See also the Committee's *Principles for enhancing corporate governance*, October 2010.

Senior Management

Principle 5: Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

Risk Management Environment

Identification and Assessment

Principle 6: Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.

Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

Monitoring and Reporting

Principle 8: Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

Control and Mitigation

Principle 9: Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

Business Resiliency and Continuity

Principle 10: Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Role of Disclosure

Principle 11: A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

---

[12] "Risk appetite" is a high level determination of how much risk a firm is willing to accept taking into account the risk/return attributes; it is often taken as a forward looking view of risk acceptance. "Risk tolerance" is a more specific determination of the level of variation a bank is willing to accept around business objectives that is often considered to be the amount of risk a bank is prepared to accept. In this document the terms are used synonymously.

Source: Principles for the Sound Management of Operational Risk. (2011). [PDF] Bank for International Settlements p.5-6.

Appendix 2: Art. 92, 93 and 94 Capital Adequacy Ordinance (CAO)

ARTICLE 92 Basic Indicator Approach

1 The minimum required capital shall correspond to 15% of the average of the earnings indicators of the three previous years. Only years with positive earnings indicators shall be taken into account.

2 The FINMA may subject the use of the basic indicator approach to additional qualitative risk management requirements.

ARTICLE 93 Standard Approach

1 The minimum required capital shall be calculated as follows:

a. For each business line and for each of the three previous years an earning indicator has to be determined and multiplied by the factor specified in (2).

b. The resulting values shall be added up for each year. In doing so, negative values from certain business lines may be netted with positive values of other business lines.

c. The minimum required capital shall correspond to a three-year average. When calculating the average, any negative sum shall be set to zero.

2 Business activities shall be assigned to the following business lines and multiplied by the following rates:

a.	Corporate finance/consulting	18%
b.	Trading	18%
c.	Private banking	12%
d.	Commercial banking	15%
e.	Payment operations / securities clearing and settlement operations	18%
f.	Custodial and fiduciary transactions	15%
g.	Institutional asset management	12%
h.	Brokerage business	12%

3 The FINMA may subject the use of the standard approach to additional qualitative risk management requirements.

ARTICLE 94 Institution-specific Approaches (AMA)

1 Banks may use an institution-specific approach (AMA) to determine the minimum required capital.

2 The FINMA shall approve the use of the AMA if the bank has a model allowing it to quantify operational risks using internal and external loss data, scenario analyses as well as key factors of the business environment and of the internal control framework.

Source: Ordinance on Capital Adequacy and Risk Diversification for Banks and Securities Dealers. (2017). [PDF] KPMG, pp.37-38.

Appendix 3: Business lines allocation for the Standard Approach (SA, Art. 93 CAO)

i	Business line	βi
1	Corporate finance / advisory	18%
2	Trading and sales	18%
3	Retail banking	12%
4	Commercial banking	15%
5	Payment and settlement operations	18%
6	Custodial and fiduciary transactions	15%
7	Institutional asset management	12%
8	Retail brokerage	12%

Source: Circular 2008/21 Operational Risk – Banks. (2016). [PDF] KPMG, pp.7.

Appendix 4: Illustrative key risk indicators

Operational Risk Source	Key Risk Indicators
People Related	Significant number of excesses and exceptions.
	Significant number of limit and financial power violations.
	Staff absenteeism and sickness rate.
	Adverse age profile of executives.
	Disproportionate number of staff disciplinary cases.
	Clubbing of conflicting responsibilities.
Operations Related	Unreasonable transaction–staff ratio.
	Significant number of unpaid clearing checks.
	Unreasonable number of debits to suspense accounts.
	Frequent entries in staff deposit accounts.
	Rapid increase in number of loan accounts.
	Significant number of large exposures.
	Frequent revisions in credit rating of borrowers.
	Large number of dematerialized accounts.
	Significant arrears in renewal of revolving credit accounts.
	Increasing incidence of nonperforming loans and advances.
	Frequent devolvement of off-balance-sheet liabilities.
	High number of speculative transactions in treasury department.
Process Related	High proportion of incomplete and expired loan documents and agreements.
	Disproportionate number of unreconciled entries in books of accounts.
	Significant variation in internal credit rating and external agency rating of same borrowers.
	Frequent defaults or omissions in capturing and entering data in the management information system.
	Disproportionate number of unsettled suit filed cases.
	Disproportionate number of written-off cases.
	Screening system not capturing suspicious transactions or money laundering attempts.
Systems Related	Unusual duration of systems downtime.
	Frequent violation of security codes in accessing computer systems.
	Number of outages in network functioning.
	Number of virus-related incidents.
External Events Related	Number of occasions burglaries took place or attempts made.
	Number of occasions when vendors/service providers failed to honor agreements/commitments.
	Number of times utility services broke down.

Source: Ghosh, A. (2012). Managing risks in commercial and retail banking, pp.420.

Appendix 5: Interview with Antoine Spinelli (BIC-BRED Suisse SA)

Interview date:	Monday April 23rd, 2018
Company:	BIC-BRED (Suisse) SA
Interviewee:	Mr. Antoine Spinelli
Title:	Chief Risk Officer
Interviewer:	Romain Gimblett
Interview conditions:	In person, no voice recorder

1. **Quel est le risque opérationnel le plus conséquent, en termes de perte estimée, au sein de votre entreprise ?**

   Mr. Spinelli : La fraude est le risque numéro 1. Il est nécessaire d'avoir une expertise du personnel pour mitiger ce risque. La Blockchain par exemple, basée sur un historique de transaction, peut aider à réduire ce risque. Ce n'est toutefois pas une solution universelle et cette technologie n'exclut pas que la transaction soit rentrée faussement.

2. **Selon vous, quel est l'impact actuel et quel sera l'impact futur de la digitalisation sur les risques opérationnels et sur le processus de gestion de ces risques ?**

   Mr. Spinelli : Cela dépendra de la capacité des outils à servir le métier. Le but serait de simplifier les tâches et assister l'environnement de contrôle. Cela permettrait de minimiser les risques grâce à un environnement de contrôle automatisé performant et efficient.
   On peut imaginer des Dashboard avec un flux d'informations entrantes en continue. Grace à cela, les managers n'auront quasiment plus besoin de faire de l'échantillonnage dans tous les départements de la banque ou sur un certain nombre de transactions. C'est un travail minutieux qui prends beaucoup de temps et qui n'est donc pas aussi réactif qu'un flux continu. Un système digital n'a pas forcément besoin d'aller plus en profondeur mais il pourrait apporter plus d'exhaustivité. Le système doit également être bien connecté aux aspects fondamentaux et à tous les départements de la banque pour être sûr de ne pas passer à côté de quelque chose. J'insiste toutefois sur le fait que le digital ne remplacera pas l'intervention humaine. Peu importe la quantité de modèles automatisés, les algorithmes etc. finalement, c'est un humain qui prends les décisions et qui subit les conséquences de ses actes et décisions.

3. **Est-ce que la digitalisation du processus de gestion des risques opérationnels va modifier ou forcer une modification des principes de la FINMA et du Comité de Bâle ? (Les principes étant les 11 principes fondamentaux de la gestion des risques opérationnels du Comité de Bâle, les exigences de fond propres de la FINMA ainsi que les 6 principes d'exigences qualitatives.)**

   Mr. Spinelli : Selon moi, il n'y aurait pas nécessairement besoin d'opérer quelconques changements. En 2017, la circulaire 17/01 de la FINMA basée sur le document BCBS239 du Comité de Bâle a repris d'anciens principes de la circulaire 08/21 traitant de la gouvernance d'entreprise et y a ajouté des principes axés sur l'IT. Il est important de garder en tête qu'en suisse il y a plus de 250 banques et la taille de ces banques varie considérablement. Ces principes doivent donc suivre un principe de proportionnalité pour qu'ils soient applicables à toutes les entités et ces principes ont donc un rôle de « cadre » réglementaire pour la gestion des risques.

4. **Quels sont les points principaux à considérer pour digitaliser le processus de gestion des risques opérationnels avec succès ?**

   Mr. Spinelli : La gestion des risques pour moi est divisée en deux parties distinctes : le réglementaire et l'opérationnel. La première chose et la plus importante, c'est que le processus digitalisé ait pour but de gérer les risques de la bonne façon, en respectant la régulation. Ensuite, il doit servir un peu comme « une aide à la conduite ». Il doit fournir une certaine quantité d'informations à l'équipe qui gère les risques opérationnels afin qu'elle puisse prendre des décisions basées sur ces informations. Grace à des modèles programmés, des indicateurs ou encore des statistiques, les managers pourront prendre des décisions plus précises et plus rapides. Cela permettra d'anticiper certains évènements.

   Maintenant, je ne suis pas convaincu que le digital pourra remplacer le jugement humain. La technologie aura purement un rôle d'assistant mais pas un rôle de preneur de décision. Le digital servira à apporter l'information à l'être humain, à pré-analyser cette information, à la regrouper sur une même page mais la décision finale restera humaine. Le digital permettra un gain de temps, on n'aura plus besoin de chercher l'information, elle vient à nous, et donc augmentera l'efficacité des employés.

   Du point de vue de la réglementation, le digital permettra d'avoir un aperçu global de tout ce qui se passe au sein de la banque (grâce aux ratios par exemple) et de voir très rapidement s'il y a quelque chose d'anormal. Autant cela peut être une aide au niveau des informations quantitatives, cependant, le qualitatif ne sera pas aidé par le digital au niveau réglementaire. La chose importante est de pouvoir anticiper ce qui va se passer dans le futur proche en analysant des données du passé. Anticiper un flux de trésorerie, trouver la bonne source de

financement, anticiper les contrôles à mettre en place et savoir si des mesures doivent être prises.
Il faudra analyser des Big Data afin de créer un modèle prédictif fiable. Cela permettra de créer des tendances et si le système décèle des données présentes qui ne correspondent pas aux tendances passées, il pourra lancer une alerte aux managers. Ils sauront exactement où mettre leurs contrôles en places pour gérer le risque à la source et au plus vite. La qualité de l'information est clé, c'est ça qui déterminera un bon système technologique.

5. **Quel sera l'impact d'une telle digitalisation sur le rôle de l'être humain dans le processus de gestion des risques ?**

Mr. Spinelli : Comme dit dans le point 3, le digital va aider l'humain à prendre des décisions. Il va lui faciliter la vie, lui apporter ce dont il a besoin, des data, des statistiques etc. L'humain aura toujours le dernier mot et il prendra toujours la décision finale.

6. **Quels nouveaux risques pourraient découler de cette digitalisation du processus de gestion des risques opérationnels ?**

Mr. Spinelli : Les risques opérationnels existent et il n'y aura fondamentalement pas de nouveaux risques. Toutefois, on pourra sans doute voir une ampleur grandissante du risque cyber. Pour cela, il sera important de mettre en place un contrôle du système de contrôle au sein de la banque.

Romain : Que pensez-vous du « contagion risk » par exemple ?

Mr. Spinelli : Certes les banques sont interconnectées et le seront probablement plus dans le futur. Toutefois, je pense que les banques ne sont pas assez interconnectées pour qu'il y ait une disruption totale de l'industrie bancaire en suisse. J'insiste sur le fait qu'il est important de rester dans son propre environnement, de faire développer notre infrastructure de notre côté et d'éviter les risques. Il faut trouver l'équilibre entre l'efficacité que peut apporter la technologie et les risques qu'elle peut causer.

Appendix 6: Interview with Yves Keller (GS Banque)

Interview date:	Wednesday April 25th, 2018
Company:	GS Banque
Interviewee:	Mr. Yves Keller
Title:	Chief Financial Officer / Chief Risk Officer
Interviewer:	Romain Gimblett
Interview conditions:	In person, with voice recorder

1. Quel est le risque opérationnel le plus conséquent, en termes de perte estimée, au sein de votre entreprise ?

Mr. Keller : Le risque opérationnel le plus important lié à la perte est principalement à l'origine d'une erreur humaine (mauvaise saisie, mauvaise interprétation, mauvaise compréhension). J'intègre le risque juridique dans le risque opérationnel car c'est un élément important dans le secteur bancaire. Un risque juridique peut avoir un impact sur l'image de la banque. C'est un risque inhérent de par l'exposition de la banque. J'exclus toutefois les risques de conformités et légaux quand j'évoque les risques opérationnels.
A l'interne de la banque, il y a des structures, des flux, qui sont souvent très systématiques, des systèmes bancaires bien carrés avec des saisies et des validations. On a des tubes qui sont bien alignés mais souvent il faut « l'input » de l'humain. La fraude est un risque séparé de l'erreur humaine bien qu'elle soit forcément faite par l'humain. Une banque peut être soumise au risque de fraude externe pour des raisons de corruptions dans certains pays. Toutefois, il faut une grosse collusion pour qu'une fraude interne ce passe.

Romain : Est-ce que vous faites des prédictions quantitatives des pertes potentielles liées à l'erreur humaine ?

Mr. Keller : Non je ne le fais pas. Les pertes opérationnelles liées à l'erreur humaine ne sont pas prédites. Elles sont généralement trop petites pour cela et c'est difficile à chiffrer. Cependant, des limites sont mises en place et si elles sont atteintes, des mesures sont prises. La banque n'a pas de modèle sur les risques opérationnels qui va déterminer le coup du capital. C'est simplement un pourcentage des revenues sur les 3 dernières années.

Romain : Pensez-vous que l'on pourra modéliser cela à l'avenir ?

Mr. Keller : Oui bien sûr ! Ce qui est intéressant, c'est qu'on va pouvoir modéliser cela à l'avenir. Pour moi, la détermination du capital devrait être beaucoup plus granulaire (pas seulement un pourcentage des revenus). Il faudrait prendre l'historique des pertes, l'occurrence des pertes et la mettre en perspective par rapport aux revenus et ce n'est clairement pas 10% des revenus qui sont des

pertes (c'est vraiment une vision très prudente du risque opérationnel, pour une banque de gestion privée). Pour du « Trade finance », le risque opérationnel est un peu négligé selon moi, car il est beaucoup sujet à fraude. En tout cas, le risque de fraude externe est beaucoup plus important. Ça arrange donc bien cette industrie que l'on base simplement le capital sur un pourcentage du revenu.

2. **Selon vous, quel est l'impact actuel et quel sera l'impact futur de la digitalisation sur les risques opérationnels et sur le processus de gestion de ces risques ?**

Mr. Keller : Aujourd'hui il y a déjà beaucoup d'outils automatiques qui permettent de suivre les risques opérationnels. Ces outils permettent de récolter des informations, de les centraliser, de les projeter en fonction du coût du capital et de les « monitorer ». Tout cela existe déjà au niveau du suivi du risque opérationnel. L'intérêt de la digitalisation est en amont de ces informations, en agissant sur les flux. Le facteur humain est l'élément qui cause le plus fréquemment des risques opérationnels, sans parler des risques juridiques, bien que, la plupart du temps, un risque juridique découle d'une mauvaise interprétation ou mauvaise action d'un humain. Le fait d'avoir des processus plus automatisés, plus digitaux, permettra de limiter le risque de facteur humain. Cependant, cela peut augmenter le risque résiduel. Si les flux ne sont pas bien dessinés, cela peut créer de gros risques.

Romain : Qu'entendez-vous par « flux » ?

Mr. Keller : Je parle des processus en amont. La gestion des risques opérationnels s'agit principalement d'identifier les risques de pertes. Ce risque de perte provient de différent facteurs. Cela peut venir d'un processus mal conçu, défectueux. Par exemple, le contrôle d'une validation devait avoir lieu mais il n'a pas été fait et finalement la banque est exposée et une perte en découle. Ou bien, une personne n'a pas bien effectué son travail et une perte en découle. Si on travail en amont de cela, la banque parviendra à réduire le risque opérationnel. La digitalisation moi j'y crois mais plus spécialement en amont, sur les flux. Dans le futur, un module de risque opérationnel sera greffé au logiciel bancaire intégré. Ce module ira chercher des données et, selon des hypothèses, il va déterminer ou identifier des transactions qui sont anormales, qui n'auraient peut-être pas dû être faites ou qui sont inhabituelles et qui permettent de voir si le flux de la banque fonctionne bien. La digitalisation va être très utile pour cela.

Romain : Cela évitera donc de devoir prendre un certain nombre de transactions et de faire des sondages ?

Mr. Keller : Les sondages sont inutiles. On va regarder l'exhaustivité des transactions et cela permettra des contrôles exhaustifs et non pas que par sondage. On va regarder toutes les opérations, si elles sont faites à des heures précises, si elles ont des chiffres bizarres ou si elles ont été saisies et validées par des utilisateurs non autorisés. Toutes ces choses permettront d 'avoir des

contrôles exhaustifs. La digitalisation, la technologie au sens large, va permettre d'avoir des contrôles beaucoup plus exhaustifs et pas que par sondage.

Romain : La digitalisation permettra également d'avoir un flux d'information qui remonterait vers les gestionnaires de risques opérationnels ?

Mr. Keller : Oui, la digitalisation permettra également un flux d'informations instantané qui remontrait aux gestionnaires de risques opérationnels afin de pouvoir prendre des mesures le plus rapidement possible et au plus proche de l'évènement. Plus on est proche de l'évènement, plus on a de chances de mitiger la perte. C'est justement souvent ça le problème, on a les informations mais pas assez rapidement ou alors quand c'est carrément trop tard.

3. **Est-ce que la digitalisation du processus de gestion des risques opérationnels va modifier ou forcer une modification des principes de la FINMA et du Comité de Bâle ? (Les principes étant les 11 principes fondamentaux de la gestion des risques opérationnels du Comité de Bâle, les exigences de fond propres de la FINMA ainsi que les 6 principes d'exigences qualitatives.)**

Mr. Keller : Ces principes sont très larges, très génériques et permettent donc de tout faire. Après il y aura des interprétations des principes comme dans certaines circulaires de la FINMA sur le risque opérationnel, par exemple l'Annexe 3 où ils ont commencé à être beaucoup plus précis sur le risque cyber, sur les SID, sur les données identifiantes, donc sur des domaines bien spécifiques. Certains de ces principes vont prendre en compte le digital dans le futur, ça va arriver, mais cela va dépendre du rythme de l'évolution. A mon avis les principes restent très basiques et couvrent tout.

Romain : Si on imagine que la Blockchain devient quelque chose de vraiment très présent au sein des banques, est ce que cela pourrait être intégré dans un principe ?

Mr. Keller : Alors la Blockchain n'est actuellement pas présente au sein des banques aujourd'hui. La Blockchain pourrait être intégrée à un ou plusieurs principes, bien sûr. La Blockchain permettra d'accélérer les transactions, il faudra mettre en place des contrôles systèmes très robustes dès le départ afin d'éviter toutes erreurs, car corriger une erreur sur la Blockchain sera probablement très compliqué voir même infaisable. Si la transaction est simplement entre le bénéficiaire et l'émetteur, qu'il n'y a pas l'intervention d'un tiers et qu'ils sont que les deux à se mettre d'accord, le risque d'erreur est faible. Le risque sera réduit en supprimant les intermédiaires.

4. **Selon vous, quels sont les points principaux à considérer pour digitaliser le processus de gestion des risques opérationnels avec succès ?**

Mr. Keller : Pour digitaliser le processus, il faudra greffer au système bancaire interne un module qui va, en fonction des critères définis au préalable, chercher des transactions bizarres ou particulières et qui nécessitent une analyse. Cela évitera d'avoir besoin d'une personne qui remonterait ces informations. C'est vraiment en amont que ça se passe. C'est dans le système même que l'on va piocher des éléments qui peuvent déboucher ou qui ont débouché sur un risque opérationnel. On le saura de manière immédiate. Aujourd'hui dans une banque, le risque opérationnel est découvert quand la personne qui a commis une erreur l'annonce. Et c'est généralement trop tard car la perte a déjà eu lieu. L'avantage de la digitalisation est d'avoir un module qui permet d'identifier en amont, le plus en amont possible, un potentiel risque opérationnel.

5. **Selon vous, quel sera l'impact d'une telle digitalisation sur le rôle de l'être humain dans le processus de gestion des risques ?**

Mr. Keller : Le côté humain sera nécessaire pour analyser la situation de manière globale et holistique. Le système va nous donner des indicateurs, une personne codera le modèle selon ce que la banque souhaite. La technologie donnera des informations primaires qu'il faudra ensuite interpréter. On peut avoir un système qui les interprète mais à la fin il faut aussi les mettre en perspective de quelque chose et pour cela il faudra l'humain (ex : la transaction est effectivement anormale mais dans les conditions XYZ on peut l'accepter).
Il y aura cependant moins besoin de personnes qui font du « data crunching » car ce seront des systèmes technologiques ou d'autres outils qui viendront se greffer au logiciel bancaire existant et qui nous donnerons ces informations primaires pour une analyse de valeurs, sur le pourquoi du comment et pas seulement la quantité.

Romain : Ça sera une utilisation de ratios par exemple ou des Dashboard avec des informations clés ?

Mr. Keller : Cela existe déjà.

Romain : Mais avec des informations ou des ratios en live ?

Mr. Keller : Ce qui est plus important outre que les ratios ou le volume, c'est les opérations ou les transactions spécifiques qui représentent une menace ou qui sont anormales car un risque opérationnel c'est souvent le résultat d'une erreur dans une transaction, pas parce qu'on fait trop de crédits. C'est parce qu'on a mal fait un crédit, ou une opération. C'est vraiment en amont, lorsque le système détecte une anomalie de traitement que l'on va pouvoir agir.

6. **Selon vous, quels nouveaux risques pourraient découler de cette digitalisation du processus de gestion des risques opérationnels ?**

Mr. Keller : Le risque de contamination et le risque cyber existent déjà aujourd'hui et ne devraient pas nécessairement prendre une plus grande ampleur en termes d'impact ou de probabilité d'occurrence.
Si on prend la technologie Blockchain, tout le monde peut avoir accès au grand livre et c'est très transparent, ça n'augmente pas nécessairement le risque. Cela dépend vraiment de la façon dont on perçoit le risque, comment on le traite et comment on le gère et comment on gère nos données. Ce sont des risques déjà avérés aujourd'hui. Si on prend la digitalisation comme des systèmes d'intelligence qui se greffent au module général de la banque, cela n'implique pas de tierces parties, c'est isolé. Si on commence à ouvrir les accès à nos informations, cela risque d'être plus compliqué.
Il faut trouver un bon équilibre à cela et c'est déjà le cas aujourd'hui. Les données ne sont pas mises dans un coffre-fort car on a besoin de ces informations pour travailler, mais si demain on fait du business basé sur une Blockchain, il faudra adapter notre système de mitigation et d'accès aux informations ou autre. Ça va s'adapter en fonction de l'avancée de l'industrie et des pratiques. Si c'est plus axé sur le digital, on sera peut-être plus exposé qu'aujourd'hui et le risque sera peut-être plus conséquent, mais on fera aussi différemment pour gérer ce risque donc finalement, la conséquence ne sera pas plus importante, le risque résiduel ne va pas nécessairement augmenter, proportionnellement ça sera la même chose.
Je pense que la digitalisation a un effet positif sur la gestion des risques opérationnels, c'est comme ça que je le vois. C'est plus facile de corriger une situation quand elle est toute récente que quand elle est antérieure.

Appendix 7: Survey – Yves Keller GS Banque

1) Quelle est la source de risque opérationnel la plus importante au sein de votre entreprise? (1 réponse possible)

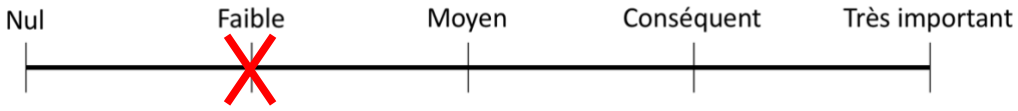
- Les systèmes
- Les processus
- Les personnes
- Les évènements externes

Remarques (optionnel) :

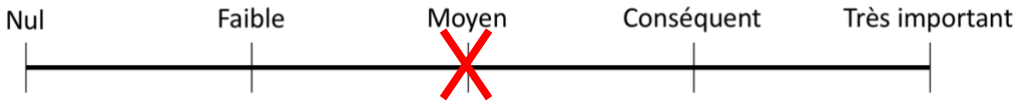
Un événement extérieur a le plus gros impact financier. Cependant le risque des personnes reste celui le plus fréquent.

2) Selon vous, quel est l'impact ACTUEL de la digitalisation sur les risques opérationnels et sur le processus de gestion de ces risques ? (1 réponse possible par échelle)

Les risques :



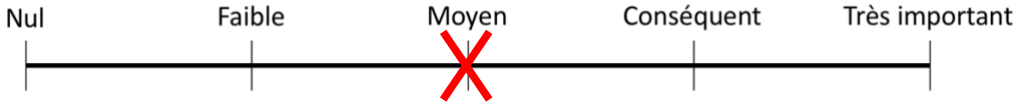
Le processus :



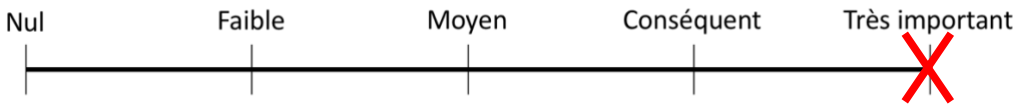
Remarques (optionnel) :

3) Selon vous, quel sera l'impact FUTUR de la digitalisation sur les risques opérationnels et sur le processus de gestion de ces risques ? (1 réponse possible par échelle)

Les risques :

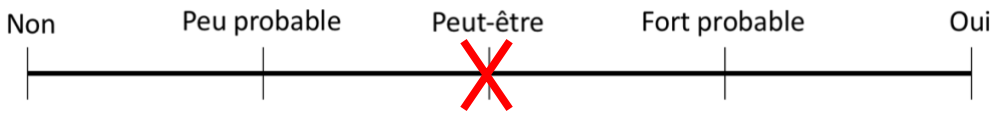


Le processus :



Remarques (optionnel) :

4) Selon vous, est-ce que la digitalisation du processus de gestion des risques opérationnels va forcer une modification des principes de la FINMA et du Comité de Bâle ? (Les principes étant les 11 principes fondamentaux de la gestion des risques opérationnels du Comité de Bâle, les exigences de fond propres de la FINMA ainsi que les 6 principes d'exigences qualitatives.)
(1 réponse possible)



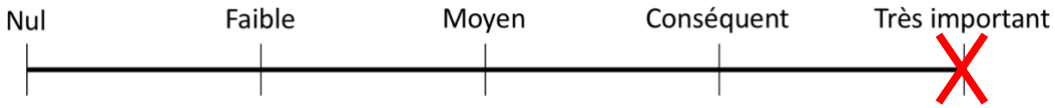
Remarques (optionnel) :

5) Selon vous, quels sont les points principaux à considérer pour digitaliser le processus de gestion des risques opérationnels avec succès ? (Plusieurs réponses possibles)

- La gestion des données
- Automatisation du flux de travail et des processus
- Analyses avancées et automatisation de la décision
- Une infrastructure cohérente et flexible
- Utilisation de visualisation intelligente et d'interfaces (ex : Réalité Augmentée)
- Un écosystème externe à la banque (ex : partenariat avec des FinTechs externes pour améliorer la détection de fraude des clients de la banque)
- Acquisition de talents et une bonne culture d'entreprise
- Aucun de ces points
- Autre :

Remarques (optionnel) :

6) Selon vous, quel sera l'impact d'une telle digitalisation sur le rôle de l'être humain dans le processus de gestion des risques ? (1 réponse possible)
Sur cette échelle, « très important » signifie que l'humain sera remplacé par des machines, « nul » signifie que la digitalisation ne remplacera en aucun cas (même pas partiellement) le rôle de l'humain et les tâches effectuées par ce dernier.



Remarques (optionnel) :

7) Selon vous, quels nouveaux risques pourraient découler de cette digitalisation du processus de gestion des risques opérationnels ?

1. …….
2. …….
3. …….

Si vous n'avez rien répondu sur les 3 espaces si dessus pensez-vous que : (1 réponse possible)

- Les risques opérationnels existent tous aujourd'hui et il n'y en aura pas de nouveaux.
- Il n'y aura pas de nouveaux risques opérationnels mais leur impact peut changer.
- Il n'y aura pas de nouveaux risques opérationnels mais leur probabilité peut changer.
- Il n'y aura pas de nouveaux risques opérationnels mais leur impact et leur probabilité peut changer.

Quels risques sont les plus susceptibles de voir leur impact / probabilité changer ?

1. Le risque humain
2. Le risque d'incohérence des données
3. …….

Remarques (optionnel) :

Appendix 8: Interview with a person from UBS Switzerland

Interview date:	Monday May 1st, 2018
Company:	UBS Switzerland AG
Interviewee:	Anonymous
Title:	Not disclosed
Interviewer:	Romain Gimblett
Interview conditions:	On the phone, no voice recorder

1. What is most important operational risk, in terms of estimated loss, faced by your firm?

The person from UBS: There are three things to consider when you look at operational risks.
One of them is regulations. Regulations are usually a bit slower then developments. We can see a time lag of 10-12 years. For example, the current regulation addresses mistakes that banks have made during the financial crisis. With this new regulation, banks must apply and implement the new requirements even though it's 10 years later. The regulation is based on historical facts, they don't anticipate the future. It shouldn't be that way according to me, however that's how it works at the moment. The market is usually quicker than the regulators by developing new models.
This brings us to our second point where operational risks may come from. If you do something that you have not done before, you may, or you may not encounter risks. Some of the risks are known because you look into the past, some of them may not be seen because they are new. If we take the example (not recent but pretty clear) of e-banking, from the banks' point of view, it is nothing more than the client doing several tasks by himself instead of going to a branch or sending a form to the bank. The transaction remains exactly the same, but you do it in a different channel. Now, this channel represents new risks to the bank as the customer enters the information by himself and it could be badly entered, it could be wrong information, or it could be information that the bank may not be able to process. This problem was not there before as the information would be entered by an UBS employee, a professional. That was a new risk for UBS at this point. A risk of fraud can also be considered in this case as you have to trust the log in system to make sure that indeed, it's Mr. XYZ that enters his account and not someone else. The changes, the new systems or the new products, changes the risk patterns. This change is continuous and represents a risk by himself.
The development of digitalization will cause that at some point, there will be no more interaction with the person cashing in and the person cashing out. Moreover, if you imagine that there is no cash anymore but only cryptocurrencies, who does guarantee that if you own 1 bitcoin (for example), that you really have 1 bitcoin? And who guarantees that this bitcoin is still valid tomorrow as it is today? These are examples where risks may come from in the future.

The third part of operational risks in banks is the human workforce. Indeed, banks have very robust and reliable systems and processes in the base lines for payment execution, operations and transactions. They have been implemented and improved with the time and thanks to these, the operational risk is very little. The real operational risk is linked to the human interface. If you could digitalize everything and you assume that the digitalization has been done correctly, because digitalizing a function means that someone needs to define what is right and what is wrong, the remaining operational risk would only be coming from the human being. Therefore, it is imperative for a bank to make sure that models, robots or any programmable technology are well coded and built from day 1 in order to mitigate the risks and avoid a loss due to an error. To link this back to regulations, every change that you must undertake because of regulators implies a thorough review of the processes and the systems to make sure that they comply to the new regulations but also that it works properly. It is mainly the external sources that change your business model, that change the way you operate or work. This is all changing your operational risks, it can enhance them or decrease them. It affects the impact and the probability of current risks if you amend a current process or system, but it can also bring new risks in the case where you would use new processes or systems.

2. **According to you, what is the actual impact and what would be the future impact of digitalization on operational risks and on the operational risk management process?**

The person from UBS: The actual impact is what we discussed under point 1. For the future impact, I see 2 folds. On one side you have processes that you have to change, and on the other side, you might miss out on things that you do wrong because everything is going a lot faster with the digitalization. For example, in the early days, you had cashier systems. Everyone having a cashier system was able to physically touch and count the bills that you had in the system. At the end of the day you summed all the bills that you had in all the cashier systems and you knew what you had on the balance sheet. Today, you have many more transactions that are also more complex. Less than 5% of what flows around the world is cash bills, the rest is some sorts of digital transactions. The daily world FX trade is a volume of about $3 trillion. If we would imagine stopping all the flows during the day and trying to reconcile every trade worldwide with every bank. Can we be sure that the balance is offsetting perfectly to have 0 on both sides? We are not sure, we only assume it. It goes so fast and it is continuously running like that. This brings me to the point that these operational risks need a margin of error. Within that margin of error, you are able to limit your risk in the sense of: “it’s ok if 10% of the trades are not settled, then we just lose 10% of capital, we can live with that”. However, what if in these 10% there is a trade with a size so huge that it could put down the whole company. This is a different kind of risk. In addition to this, you really have to bear in mind the velocity of transactions and the velocity of processes and changes in the system. The important thing to ask is: “Can operational risk management process even look at these details, is it granular enough?” It is worth noting that the process must

be granular enough to spot the small details while still being able to let the transactions flow through. If you want 0 risk you just stop the business, avoidance is the best risk strategy to have actually no risk. You need a margin of error, a residual risk that you can live with and that you're happy to accept if things go sour, to still be able to do business.

As digitalization happens, you have to adapt your operational risk management process, however, digitalization may also be used in the operational risk management process (robots, big data). If we take the example of the fraud prevention at a credit card company, they have algorithms that we can consider as a robot. This robot does nothing else that looking at patterns (spending patterns, geographical patterns). The Big Data chunk can help you to find risk. In the same way, it is also a risk in itself because when you look at data you always look backwards, you look at past happenings. So, if someone wants to fraud the system, if they are aware of how and why you use the data and what data you are using, they can also use the same data to hack you or make a fraud. Digitalization means that you also need to be very protective, from the external actors and environment, on how you use data and what type of data you use as input. You really have to find the right balance between leveraging the data and exploiting it and being hacked or that somebody else uses the same information. If you look at people investing in quantitative models, you have no clue of how the money is made. The funds give you hints on how it works but if they gave you all the details, they would just give out their secret recipe.

3. **Will the digitalization of the operational risk management process modify or imply a modification of the principles of the FINMA and the Basel Committee (BCBS)? (The principles being the 11 Principles for the Sound Management of Operational Risk and the Role of Supervision of the BCBS, the Capital Adequacy Requirements and the 6 qualitative requirements on handling operational risks of the FINMA)**

The person from UBS: The FINMA principles will have to change, they will need to adapt. For example, if people don't use credit cards anymore but just use systems as Twint, they might need to adapt.
If you look at the Basel capital requirements, what if a bank starts doing business in an area where there is no capital needed? If you only do transactions, there is no capital needed, you need to have running capital, but you don't need any underlying capital. AliPay, Apple Pay are not banks, they purely do transactions and you need a bank account to settle the transactions against. Now you have two providers doing what one entity was doing before. The fragmenting of the value chain can also lead to risk. You have the transfer risk between the different providers, you are not sure if everyone in the value chain is under the same regulations. FINMA and BCBS must take this in the consideration in the future.

4. **What are the major factors / key points to take into consideration to digitalize successfully the operational risk management process?**

   The person from UBS: You need to know where your data is. You need to know how to process and analyse the data. You need to know how the business model can change or will change. If you have these factors you can actually work on it. I am confident that whatever operational risk framework you build, the risk is usually there first. What would be really new is to have a model that can estimate whatever risk could arise before you even encounter the risk. This would be very powerful. This is a long shot, but this would be a very new approach to operational risk management.

5. **What will be the impact of this digitalization on the role of human beings in the operational risk management process?**

   The person from UBS: I think that nowadays, you have people that make the framework, you have people that make the controls and you have people that make the analysis. I think that in the future you will still have the people making the frameworks because the machine will not be that intelligent. The people who make the controls will be replaced partially to a big extent. You will need people that can calibrate the robot or the machine. It will be maintenance but not only. These people will need to think for the machine as robots and machine can only think and do what you tell them to think and do. Artificial intelligence, I don't buy it, that's in movies. I don't think that this is really going to happen. The machine is always as smart as the person which programs the machine. It is possible that the models can start reshaping themselves for a bit. I think that in terms of controls, the machine can give the human beings data and information to react on (estimate risk or predict it for the future), it will have a role of assistant, there will still be a human intervention to take decisions and decide on what to implement. I don't think that any regulator would allow a machine to handle the risks by itself and make the decisions out of the risk controls. This might happen in the next 40-50 years but not before. In the next 10-20 years, first of all the human being doesn't like to be replaced, secondly, who would program that machine? If I am managing my own risks, would I really rely on a third party telling me that I have a machine and that it takes action without being told what it is exactly doing, what if something goes wrong? At the end of the day, the human being is the one liable if things go sour.

6. **What new risks could arise from the digitalization of the operational risk management process?**

   The person from UBS: As I mentioned before, you might have data that you can use for the risk management process however this data may also be used against you and this is a clear threat. If you look at the anti-virus companies, they employ hackers, the employ criminals. Why? Because these guys are on both sides. Digitalization offers worldwide data owned by worldwide companies that influence what you implement in your operational risk management system.

In the early days it was a human being that was sitting there and counting bills or thinking on how you can control the person counting bills or how often does this person need to count the bills. This was kind of independent, you needed to know someone and have his trust to make him commit a fraud. With the digital system you can sneak in from a completely different angle. You can use the data to do so, you can fraud the data, you can modify the data streams, you can reprogram or program badly the digital tools on purpose. For example, if you have a risk management system and you know that I want to cheat on a very specific thing I can know the code as it's implemented in the system. If we go from A to B and the machine says everything is sound, do you believe the machine, or do you need someone to check and challenge how the machine came to this result?
If everybody uses the same logic and methodology, it is very easy to put everybody down. The contagion risk can be a great threat for the industry. However, I think that big banks will rely on their own model and own processes built in house and it won't rely on other models. This will mitigate in some sort the risk. For example, if you have two banks working in 2 different physical locations and they both have their servers in an identical location. If they want to reduce their costs the operational managers from both firms might consider using one company with one server for both banks. They both put their data on this server. Risk wise, not an issue. Now imagine that there is a fire exactly where the server is located. In the past, you would've had one bank down as there was only one fire in one of the banks. Now, there is a decentralized fire, not even in one of the banks, and two banks are down. It is very simple. Risk management will prioritize having your own infrastructure. However, you can read in the press, that banks are aiming at centralizing their systems. On a digitalization point of view, that works as you'll be able to access more data and more information. However, on a risk point of view, it doesn't. There is a physical risk in addition to cyber risk, such as hacking. If criminals manage to enter the centralized infrastructure, they can corrupt the whole industry or at least all the banks linked to this identical infrastructure. It goes against the principles of Blockchain as well which is currently one of the most advanced technology nowadays.

Appendix 9: Survey – A person from UBS Switzerland

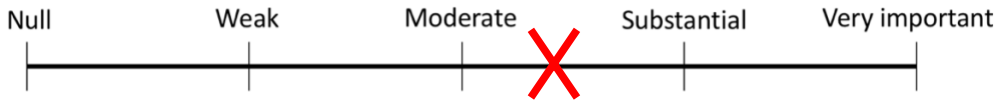
1) What is the most important source of operational risks within your firm? (1 possible answer)

- The systems
- The processes
- The people
- The external events

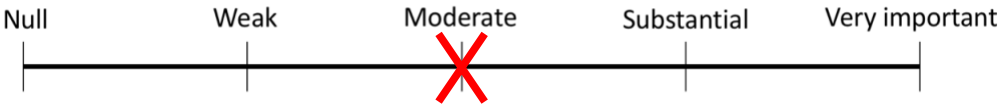
Remarks (optional):

2) According to you, what is the ACTUAL impact of digitalization on operational risks and on the operational risk management process? (1 possible answer per scale)

The risks:



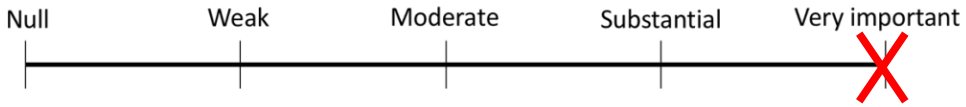
The risk management process:



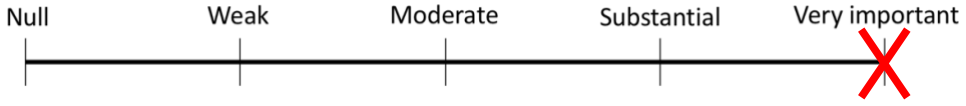
Remarks (optional):

3) According to you, what will be the FUTUR impact of digitalization on operational risks and on the operational risk management process? (1 possible answer per scale)

The risks:

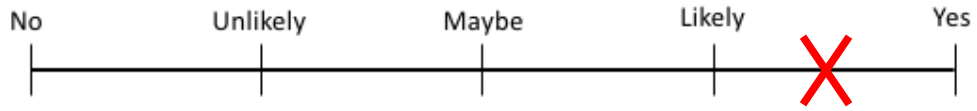


The risk management process:



Remarks (optional):

4) According to you, will the digitalization of the operational risk management process imply a modification of the FINMA and the Basel Committee (BCBS) principles? (The principles being the 11 principles of the BCBS for the sound management of operational risk, the capital adequacy requirements of the FINMA as well as the qualitative requirements for operational risks at banks)
(1 possible answer)



Remarks (optional):

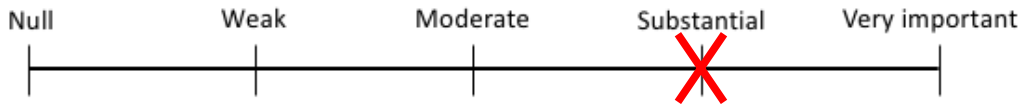
Delay in implementation of rules and regulations

5) According to you, what are the key points to consider in order to digitalize the operational risk management process successfully? (Several possible answers)

- Data management
- Process and workflow automation
- Advanced analytics and decision automation
- Cohesive, timely, and flexible infrastructure
- Smart visualization and interfaces (i.e. Augmented Reality)
- External ecosystem (i.e.: partnership with FinTech firms to improve fraud detection by the banks' customer)
- Talent and culture
- None of the above
- Other:

Remarks (optional):

6) According to you, what will be the impact of such a digitalization on the role of human beings within the operational risk management process? (1 possible answer)
On this scale, "very important" signifies that the human being will be replaced by machines, "null" signifies that digitalization will in no way replace the role of the human being (not even partially) and the tasks undertaken by the latter.



Remarks (optional):

→ Controls will be done by systems and robots
→ Systems and robots will be fed by people

7) According to you, what new operational risks could arise from the digitalization of the operational risk management process?

1. Segregation of tasks
2. Blockchain
3. Big data and similar risk system

If you didn't answer anything on the three lines above, do you think that:

- All the operational risks exist today and there will not be any new ones arising in the future
- There won't be any new operational risks, but their impact might change
- There won't be any new operational risks, but their probability might change
- There won't be any new operational risks, but both their impact and probability might change

Which risks are the most likely to see their impact / probability change?

1. .....
2. .....
3. .....

Remarks (optional):

Appendix 10: Interview with 2 people from HSBC Switzerland

Interview date:	Tuesday May 8th, 2018
Company:	HSBC Switzerland
Interviewees:	Anonymous
Title:	Not disclosed
Interviewer:	Romain Gimblett
Interview conditions:	In person, with voice recorder

1. **Est ce qu'on peut considérer une éventuelle digitalisation de la partie qualitative du processus de gestion des risques ?**

   Les personnes de HSBC : Je pense que la présence d'un être humain est nécessaire pour la partie qualitative de ce processus car il faut pouvoir faire des relations entre des données, la réalité du terrain, et puis les besoins de la banque en fonction de son appétit du risque. Cela permet de mettre en place des contrôles appropriés et de prendre des mesures adéquates. On ne peut pas faire cela uniquement basé sur des analyses de chiffres. La partie quantitative peut clairement être digitalisée à notre avis, en tout cas bien plus que le coté qualitatif, basée sur des métriques claires que l'on choisit au préalable. Par exemple, en tant que « risk manager », j'ai besoin de savoir combien de risques sont qualifiés comme moyen sur le mois actuel, combien de pertes on a eu ou combien de cas de fraudes on a eu. A partir de ces métriques-là, on a une analyse quantitative qui est déjà bien avancée, on peut ensuite procéder à l'analyse qualitative que l'on va baser sur ces métriques. Le challenge est vraiment de savoir quelles métriques ont va prendre ainsi que la qualité de ces dernières.

   Romain : C'est vrai que l'importance des données est un paramètre clé dans ces circonstances.

   Les personnes de HSBC : Ce qui est important c'est déjà de pouvoir avoir accès aux données. Si on prend notre banque comme exemple, on nous demande parfois des choses simples et très pragmatiques mais l'accès aux données pour formuler notre réponse est très compliqué. Une question de ce type peut-être : « Quel est le pourcentage de serveurs qui sont patchés en termes de vulnérabilité ? » C'est une question simple mais elle peut devenir très compliquée à résoudre car c'est très difficile d'avoir accès à ces données. En gros, plus on digitalise, plus c'est difficile d'avoir des données de qualité.

2. **Est-ce qu'on pourrait imaginer avoir un flux de données live provenant du module bancaire qui remonterait jusqu'aux risk managers ?**

   Les personnes de HSBC : En « live », non car même s'il y a un incident ou une faiblesse dans les points de contrôles que l'on a mis en place, il y a toujours l'humain qui est là pour vérifier si effectivement il y a un « deal » qui est mal passé ou si un « call-back » n'a pas été fait. Peu importe ce qu'il se passe, il y a toujours l'humain qui est là pour vérifier si c'est un faux-positif ou au contraire si c'est effectivement un risque avéré. Donc le système va nous signaler des erreurs, toutefois, il y a toujours l'humain qui est là pour vérifier ces erreurs. D'autant plus qu'après cela, il y a certaines mesures à prendre, on ne peut pas tout automatiser. Si notre système de contrôle à une faiblesse, il faut déterminer quelle est cette faiblesse et il faut y remédier au plus vite. Quelque part, chaque cas est traité différemment.

   Romain : Petite précision, qu'entendez-vous par « Call-back » ?

   Les personnes de HSBC : Lorsqu'un client envoi un e-mail pour un retrait d'argent, le « relationship manager » doit appeler le client sur le numéro enregistré à la banque afin de vérifier si c'est bien lui qui a envoyé l'e-mail et non pas un fraudeur.

3. **Quels sont les 5 risques opérationnels les plus conséquents, en termes de perte estimée, au sein de votre entreprise ?**

   Les personnes de HSBC : Les risques opérationnels ont déjà tous été identifiés et on a mis en place des « risk controls assessment ». Cela signifie que pour chaque risque opérationnel, il y a des contrôles spécifiques associés à ces risques. Par la suite il y a une évaluation qui est faite au niveau du risque inhérent, ensuite il y a certains contrôles qui vont mitiger ces risques-là, on va évaluer ces contrôles et on va finalement garder ce qu'on considère comme risque résiduel. On classifie ensuite les risques en « high-medium-low ». Selon cette classification, il va falloir mettre en place les bons processus et mettre en charge les bonnes personnes. Les personnes en charge de ces contrôles doivent les tester, les monitorer, mettre en place des KRI (Key Risk Indicators) etc.
   Cela montre bien l'importance de la partie humaine. La gestion des risques n'est pas binaire, il faut toujours avoir un œil humain pour mettre la situation en perspective et décider si oui ou non c'est un risque. Il y a des mesures qui peuvent être automatisées, les KCI, KPI et KRI par exemple. Ce sont des « Key Controls Indicators », « Key Performance Indicators » ou des « Key Risk Indicators ». Par exemples, un KCI peut nous indiquer qu'un contrôle est effectif tant que 90% des transactions sont effectuées correctement. Si la limite est passée, on reçoit une alerte, mais il faut tout de même qu'un humain recherche ce qui s'est passé afin de comprendre si c'est un problème de système, un problème de processus etc. Après cela il faut effectivement revoir l'efficacité du contrôle et peut être mettre d'autres contrôles ou mesures en place.

Romain : Par exemple une transaction pourrait être signalée à cause d'un montant inhabituel alors que dans ce cas précis elle serait valide ?

Les personnes de HSBC : Oui, ou alors dans d'autres cas une transaction n'aurait pas dû partir mais la banque a été mal informé par une tierce partie et a envoyé l'argent à la mauvaise personne. Il y a tellement de variables différentes dans tous les processus de la banque, que c'est même compliqué à chaque fois de trouver la « root cause » d'un incident qui a pu avoir lieu et de l'évaluer correctement, bien qu'il y ait des processus définis pour cela. On ne peut pas donner cela à une machine et lui demander de déterminer la « root cause ».

Romain : Est-ce qu'on pourrait considérer que dans le futur la technologie puisse aider plus l'humain dans cette détermination des « root cause » ?

Les personnes de HSBC : La digitalisation pourrait dans le cas de figure où l'on utiliserait un système où toutes les parties prenantes seraient dans le même processus au sein d'un même « workflow ». On pourrait avoir un système de vérificateurs qui permettraient de passer d'une étape du « workflow » à une autre en s'assurant que la donnée présente à un endroit X du « workflow » était correcte.
La digitalisation aura vraiment un rôle d'assistant du « risk manager », il y aura impérativement besoin de l'intervention et de la perspective humaine. Il faut vraiment un cerveau humain afin de bien comprendre l'infrastructure de la banque, les besoins, et prendre en compte les spécificités. Du point de vue des régulations, les régulateurs sont aussi plus sereins quand ils savent que certaines personnes dans la banques gèrent certains risques bien spécifiques.

4. **Selon vous, quels sont les points principaux à considérer pour digitaliser le processus de gestion des risques opérationnels avec succès ?**

Les personnes de HSBC : Avant de parler de la digitalisation du processus de gestion des risques qui comporterait de multiples facettes, il va d'abord falloir améliorer les « dashboards », les ratios, etc. que l'on utilise aujourd'hui. Il y a encore beaucoup de banques qui sont au stade de définir ce qu'elles souhaitent voir sur leurs « dashboards ». Les outils de « Governance, Risk and Compliance » (GRC) sont en constante évolution. Il n'y a pas encore de standard de norme qui définit un logiciel comme une référence reprenant tous les paramètres.
Ce qui serait vraiment nouveau et très utile, c'est un « framework » commun où toutes les personnes impliquées dans la gestion des risques, dans les contrôles associés aux risques, et dans le test de ces contrôles peuvent rentrer leurs données et consulter celles des autres. Il y a vraiment beaucoup de place pour des améliorations. On ne peut toutefois pas considérer un modèle unique qui puisse être utilisé dans toutes les banques.
La limite de la digitalisation pour nous c'est le point de la décision. Sur qui est ce qu'on va mettre la responsabilité si c'est une machine qui prends une décision ? Le « senior management » de la banque souhaite que ça soit un être humain qui

soit responsable, qui assume les conséquences, qui peut réfléchir au problème, qui a de l'expérience, qui prends en compte les changements, et qui considère l'historique de la banque ainsi que les meilleures pratiques du marché. Toutes ces choses sont à prendre en compte et sont complexes à digitaliser, à coder. On est encore loin d'être au stade où une machine peut prendre les mêmes décisions qu'un humain. Le jour où on y arrive, ça sera une autre histoire.

5. **Selon vous, quels nouveaux risques pourraient découler de cette digitalisation du processus de gestion des risques opérationnels ?**

   Les personnes de HSBC : Les risques opérationnels, à notre avis, sont tous identifiés. On n'imagine pas que dans le futur on puisse en identifier de nouveaux. On sait qu'on a des risques de « compliance », des risques de fraude, des risques « d'information security », des risques de crédits etc. Ensuite on a des facteurs externes qui vont venir influencer ces risques, par exemple, on peut avoir catégorisé un risque comme « low » aujourd'hui, mais l'année prochain il sera « high ». C'est un processus de classification continu. Les lois aussi sont des éléments externes à la banque qui influencent beaucoup la gestion des risques. On a pu voir en 2017 que la FINMA a mis à jour sa circulaire 08/21 pour que les banques intègrent le risque cyber dans leur gestion des risques opérationnels. Grace à cela, on se rend compte que les régulateurs deviennent plus regardant sur tout ce qui est cyber (qui est le « top emerging risk »). On doit donc travailler là-dessus car la loi va de plus en plus se focaliser là-dessus dans le futur. Le risque cyber ou de contamination (contagion risk) sont déjà présents, ce qui peut changer c'est l'influence du digital sur ces risques.
   Plus qu'un changement des risques, on va surtout observer un changement des contrôles. C'est déjà ce qu'on a pu observer par le passé. Par exemple, si on utilise la Blockchain, les risques ne vont pas changer mais les contrôles oui.

6. **Selon vous, quel est l'impact actuel et quel sera l'impact futur de la digitalisation sur les risques opérationnels ?**

   Les personnes de HSBC : L'impact actuel sur les risques est faible car si on nous vole des données digitales ou si on nous vole un papier, l'impact est le même. Sur le processus, l'impact est très important.

7. **Selon vous, quel est l'impact actuel et quel sera l'impact futur de la digitalisation sur le processus de gestion des risques opérationnels ?**

   Les personnes de HSBC : L'impact sur les risques sera faible comme dit précédemment. L'impact sur le processus sera très important.

8. **Est-ce que la digitalisation du processus de gestion des risques opérationnels va modifier ou forcer une modification des principes de la FINMA et du Comité de Bâle ? (Les principes étant les 11 principes fondamentaux de la gestion des risques opérationnels du Comité de Bâle, les exigences de fond propres de la FINMA ainsi que les 6 principes d'exigences qualitatives.)**

   Les personnes de HSBC : Oui, si par exemple la Blockchain devait être utilisée par les banques, elle pourrait intégrer les principes.

Appendix 11: Survey – 2 people from HSBC Switzerland

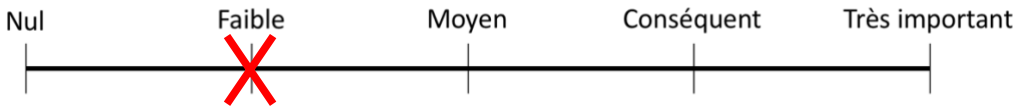
1) Quelle est la source de risque opérationnel la plus importante au sein de votre entreprise? (1 réponse possible)

- Les systèmes
- Les processus
- Les personnes
- Les évènements externes

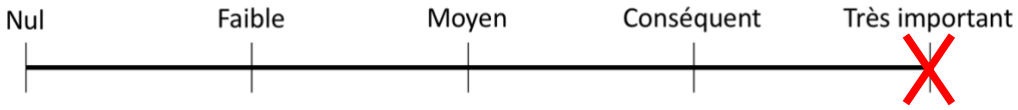
Remarques (optionnel) :

2) Selon vous, quel est l'impact ACTUEL de la digitalisation sur les risques opérationnels et sur le processus de gestion de ces risques ? (1 réponse possible par échelle)

Les risques :



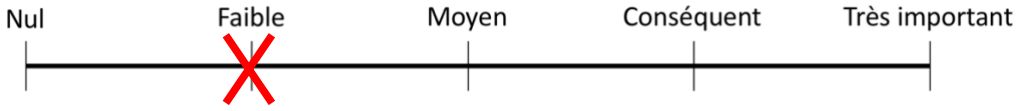
Le processus :



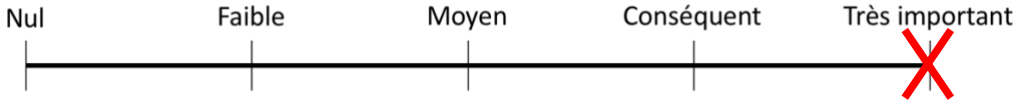
Remarques (optionnel) :

3) Selon vous, quel sera l'impact FUTUR de la digitalisation sur les risques opérationnels et sur le processus de gestion de ces risques ? (1 réponse possible par échelle)

Les risques :

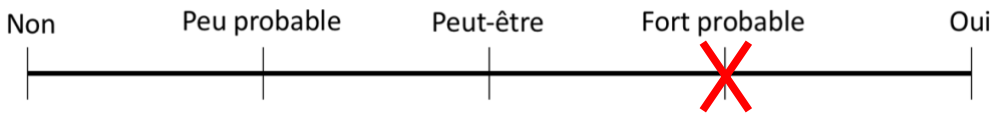


Le processus :



Remarques (optionnel) :

4) Selon vous, est-ce que la digitalisation du processus de gestion des risques opérationnels va forcer une modification des principes de la FINMA et du Comité de Bâle ? (Les principes étant les 11 principes fondamentaux de la gestion des risques opérationnels du Comité de Bâle, les exigences de fond propres de la FINMA ainsi que les 6 principes d'exigences qualitatives.)
(1 réponse possible)



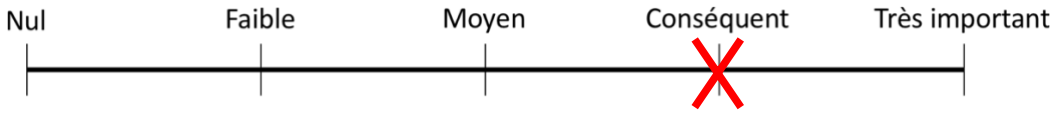
Remarques (optionnel) :

5) Selon vous, quels sont les points principaux à considérer pour digitaliser le processus de gestion des risques opérationnels avec succès ? (Plusieurs réponses possibles)

- La gestion des données
- Automatisation du flux de travail et des processus
- Analyses avancées et automatisation de la décision
- Une infrastructure cohérente et flexible
- Utilisation de visualisation intelligente et d'interfaces (ex : Réalité Augmentée)
- Un écosystème externe à la banque (ex : partenariat avec des FinTechs externes pour améliorer la détection de fraude des clients de la banque)
- Acquisition de talents et une bonne culture d'entreprise
- Aucun de ces points
- Autre : La qualité des données

Remarques (optionnel) :

6) Selon vous, quel sera l'impact d'une telle digitalisation sur le rôle de l'être humain dans le processus de gestion des risques ? (1 réponse possible)
Sur cette échelle, « très important » signifie que l'humain sera remplacé par des machines, « nul » signifie que la digitalisation ne remplacera en aucun cas (même pas partiellement) le rôle de l'humain et les tâches effectuées par ce dernier.



Remarques (optionnel) :

7) Selon vous, quels nouveaux risques pourraient découler de cette digitalisation du processus de gestion des risques opérationnels ?

1. …….
2. …….
3. …….

Si vous n'avez rien répondu sur les 3 espaces si dessus pensez-vous que : (1 réponse possible)

- Les risques opérationnels existent tous aujourd'hui et il n'y en aura pas de nouveaux.
- Il n'y aura pas de nouveaux risques opérationnels mais leur impact peut changer.
- Il n'y aura pas de nouveaux risques opérationnels mais leur probabilité peut changer.
- Il n'y aura pas de nouveaux risques opérationnels mais leur impact et leur probabilité peut changer.

Quels risques sont les plus susceptibles de voir leur impact / probabilité changer ?

1. La sécurité informatique
2. Le risque de fraude
3. Le risque de compliance

Remarques (optionnel) :